# UNIVERSIDAD AUTONOMA DE MADRID

## ESCUELA POLITECNICA SUPERIOR



**Grado en Ingeniería Informática**

# TRABAJO FIN DE GRADO

## INTEGRACIÓN DE LA NORMATIVA Y LEGISLACIÓN ACTUAL DE PROTECCIÓN DE DATOS EN EL PROCESO UNIFICADO DE DESARROLLO SOFTWARE

**Miguel Ángel Marroyo Bouzada**
**Tutora: María Elena Gómez Martínez**
**Ponente: Silvia Teresita Acuña Castillo**

**JUNIO 2020**

# INTEGRACIÓN DE LA NORMATIVA Y LEGISLACIÓN ACTUAL DE PROTECCIÓN DE DATOS EN EL PROCESO UNIFICADO DE DESARROLLO SOFTWARE

**AUTOR: Miguel Ángel Marroyo Bouzada**
**TUTORA: María Elena Gómez Martínez**

**Dpto. Ingeniería Informática**
**Escuela Politécnica Superior**
**Universidad Autónoma de Madrid**
**Junio de 2020**

# Resumen

Este Trabajo Fin de Grado consiste en el análisis de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales española, adaptando cada uno de sus noventa y siete artículos al proceso unificado de desarrollo *software*.

El objetivo principal es elaborar una guía comprensiva para un equipo de desarrollo que permita conocer los requerimientos legales de la normativa durante todas las actividades del desarrollo *software*, desde la toma de requisitos hasta la entrega al cliente y el mantenimiento. Con ello, se da respuesta al problema de la validación del cumplimiento de la ley *a priori*, dado que la mayoría del trabajo ya desarrollado se centra en el cumplimiento *a posteriori*, cuando el sistema o aplicativo ya está siendo utilizado.

La metodología desarrollada consiste en una primera lectura de cada artículo para comprender el contexto general, extrayendo una serie de términos clave que permitirán situar cada artículo en una o varias actividades del proceso de desarrollo. Después, se analiza cada artículo de forma individual para profundizar en su contenido, definiendo, si fuera necesario, nuevas palabras claves que aparezcan en él. De forma iterativa, se vuelven a comprobar todos los artículos ya tratados para validar que efectivamente pertenecen a la actividad del desarrollo indicada. En caso de que el artículo claramente no tenga cabida dentro del contexto tecnológico, se descarta anotando el motivo.

Una vez situado cada artículo, por cada una de las actividades del desarrollo *software* se detalla la forma en la que afectan los artículos y se propone la forma en la que un equipo de desarrollo deberá afrontar cada requisito técnico para cumplir con los requerimientos de la ley. Para estas propuestas se ha seguido el estándar que marca la asociación DAMA International, conocida por su guía del manejo de los datos.

Para validar esta adaptación, se ha utilizado el Listado de Cumplimiento Normativo de la Agencia Española de Protección de Datos, que, pese a centrarse en el Reglamento General de Protección de Datos, permite obtener una aproximación del porcentaje de cumplimiento *a posteriori* que se conseguiría siguiendo las indicaciones del presente trabajo.

La conclusión a la que se ha llegado con este Trabajo Fin de Grado es que la Ley Orgánica de Protección de Datos Personales tiene un importante valor dentro del sector tecnológico y la informática y por ello debe tenerse en cuenta durante todo proceso relacionado con el desarrollo *software*. Además, garantiza que, si se siguen sus indicaciones, el tratamiento de los datos personales sea transparente, honesto y seguro, lo que es de gran importancia tanto para las empresas y organizaciones como para los propios usuarios.

# Palabras clave

Dato personal, metadato, seguridad, calidad del dato, requerimiento legal, desarrollo *software*, análisis, diseño, mantenimiento, pruebas, requisito, fase, actividad

# Abstract

This Bachelor Thesis consists of the analysis of the Spanish Organic Law on Personal Data Protection and guarantee of digital rights, adapting each of its ninety-seven articles to the unified software development process.

The main objective is to elaborate a comprehensive guide that allows a development team to know the legal requirements of the law during all activities of software development, from the requirement capture to the final delivery to the client and the product maintenance. This is a response to the problem of law compliance *a priori* since most of the work already developed is focused in compliance of systems or applications that are already being used.

The methodology developed consists of a first reading of each article to understand the general context, extracting a series of key terms that will allow to locate each article in one or several activities of the development process. Afterwards, each article is analyzed individually to deepen into its content, defining, if necessary, new key word that appear in it. All the articles already discussed are checked again in an iterative way to validate that they really belong to the indicate activity. If the article clearly has no relationship with the technological context, it is discarded noting the reason.

Once each article has been placed, for each of the activities of development, the way in which the articles affect it is detailed and the way in which a development should deal with each requirement in order to comply with the law is proposed. For these proposals, the standard set by the DAMA International association, known for its data management guide, has been followed.

To validate this adaptation, the List of Regulatory Compliance of the Spanish Data Protection Agency has been used, which, despite focusing on the General Data Protection Regulation, allows an approximation of the percentage of compliance that would be achieve following the indications of this work.

The conclusion reached with this Bachelor Thesis is that the Organic Law on Personal Data Protection has an important value within the technology sector and therefore must be considered during all processes related to software development. Furthermore, it guarantees that, if its indications are followed, the treatment of personal data is transparent, honest and secure which is of great importance for companies and organizations as well as for the users themselves.

# Keywords

Personal data, metadata, security, data quality, legal requirement, software development, analysis, design, maintenance, test, requirement, phase, activity

## *Agradecimientos*

***A mis padres, mi hermana y a mi tutora Elena por toda la ayuda y tiempo dedicado a este trabajo.***

# ÍNDICE DE CONTENIDOS

# ÍNDICE DE FIGURAS



# ÍNDICE DE TABLAS

# 1 Introducción

## 1.1 Motivación

En mayo de 2018 entró en vigor en la Unión Europea el Reglamento General de Protección de Datos [1], en adelante RGPD, el cual supone un gran avance en cuanto a la protección de datos personales. Este reglamento implica para las empresas de la Unión Europea, o aquellas que trabajen con datos de residentes en ella, un nuevo desafío a cumplir para evitar las costosas multas (de hasta 20 millones o un 4% del volumen de negocio) y ofrecer a sus clientes un servicio que garantice sus derechos de privacidad. En España, dicho reglamento se ha adaptado a las necesidades nacionales con la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales [2], en adelante LOPDP, que entró en vigor en mayo de 2018.

En 2017, en una encuesta realizada por PwC [3], un 92% de las organizaciones de los Estados Unidos de América consideraba que, pese a ser una normativa europea, afectaría a su negocio y por lo tanto el cumplimiento debía ser una prioridad. En ese mismo año, Deloitte condujo una encuesta [4] a organizaciones en EMEA (Europa, Oriente Medio y África) en la que solo un 15% de las empresas consideraba que para mayo de 2018 podría cumplir totalmente la normativa. Hasta la fecha, junio de 2020, empresas como Facebook o Google han recibido multas por valor de 114 millones de dólares y países como Grecia, Portugal o Eslovenia todavía no han adaptado las medidas a sus normativas nacionales [5]. Por ello, pese a la reconocida importancia que tiene el reglamento, queda en evidencia que aún no se está actuando plenamente para cumplir con él.

Dentro del contexto tecnológico, uno de los pilares fundamentales de cualquier aplicación o sistema informático son los datos. Se entiende como dato aquella información que se almacena de forma digital y como dato personal toda información de una persona física que permita identificarla.

*"datos personales es toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona."*

Artículo 4 - RGPD

Un dato es una forma de representación de la realidad que normalmente carece de contexto y que debe ser interpretado para tener un sentido y poder ser una fuente de información. Además de representar la realidad, también se pueden representar a los propios datos sobre la misma. Para ello existen los metadatos, datos sobre los datos, que permiten conocer información sobre ellos. Un ejemplo sería el de un fichero informático en él se almacenan los datos sobre los productos. Los datos propios sería el contenido del fichero mientras que la información que describe al fichero en sí (nombre, tamaño, etc.) serían los metadatos. En la Figura 1 se muestra un ejemplo de metadatos de un archivo Word.

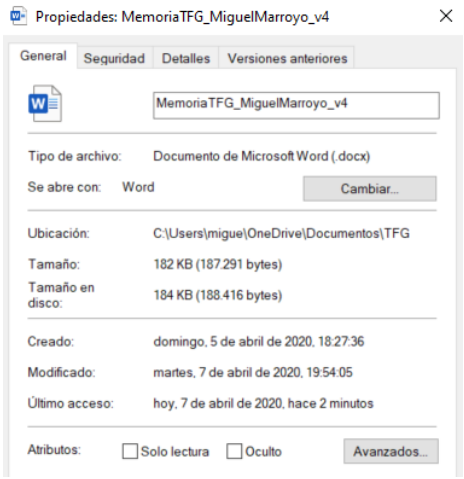


**Figura 1. Ejemplo de metadatos de un archivo Word**

Hoy en día, muchas empresas tienen como principal forma de ingreso servicios relacionados con los datos, desde su tratamiento hasta su distribución a terceros. Por tanto, el dato ha pasado a considerarse como un activo, que se utiliza para producir valor o que cuenta con él de forma intrínseca. Además, los sistemas de información se basan en su mayoría en el manejo de datos, sin ellos las empresas no podrían contabilizar su *stock*, el Gobierno no podría identificar a los ciudadanos o Facebook no recordaría el cumpleaños de sus usuarios. Por este motivo, surge la necesidad de regular las actividades que los involucren, con el fin de proteger a los usuarios frente a un mal uso de sus datos personales, garantizando unos niveles de seguridad y transparencia adecuados.

## 1.2 Objetivos

El objetivo de este trabajo es estudiar y analizar los artículos de la LOPDP española, sintetizando todos sus requerimientos, obligaciones y condiciones, y poniéndolos a la par con el Proceso Unificado de Desarrollo *Software* [6], en adelante PUDS, con el fin de crear una guía comprensiva para un equipo de desarrollo que le permita conocer los requisitos necesarios que tener en cuenta para cumplir con los requerimientos legales del reglamento.

Las fases del proceso unificado que se han tenido en cuenta son: inicio, elaboración, construcción y transición. Cada fase se divide en iteraciones y consta de disciplinas, que son un conjunto de actividades, de las que destacan: toma de requisitos, análisis, diseño, codificación o implementación, pruebas y mantenimiento. Sobre el conjunto de disciplinas o actividades es sobre donde se ha realizado la tarea de situar cada uno de los artículos. El trabajo se ha centrado en las fases técnicas del desarrollo y no en los procesos de gestión.

Para ello, se ha analizado de forma manual cada uno de los noventa y siete artículos principales que componen la ley, buscando palabras clave que permitan decidir en qué momento del desarrollo de una aplicación se debería tener en cuenta dicho artículo. Se ha desarrollado de forma manual debido a la naturaleza judicial del reglamento, que en muchas ocasiones requiere del contexto general para poder interpretar la ley de forma correcta. Además, el conjunto de palabras clave no está establecido *a priori* ya que el reglamento no tiene por qué contener palabras relacionadas con procesos tecnológicos, por lo que se justifica el análisis manual. Muchos de estos artículos se deberán tener en cuenta durante varias de las actividades, por lo que han sido tratados desde el punto de vista relativo a cada una, con el fin de que se pueda garantizar su cumplimiento total.

## 1.3 Organización de la memoria

La memoria de este Trabajo de Fin de Grado consta de los siguientes capítulos:

En el Capítulo 2, Estado del Arte, se analizan brevemente las soluciones propuestas hasta la fecha para el cumplimiento de la normativa y se comparan con el presente Trabajo de Fin de Grado, confirmando que hasta la fecha todavía no se ha desarrollado ningún trabajo con el mismo punto de vista.

Marco Teórico, tratado en el Capítulo 3, en el que se introducen los puntos clave necesarios para comprender los fundamentos del RGPD y la LOPDP, el Esquema Nacional de Seguridad [7], las fases y actividades del Proceso Unificado de Desarrollo y los principales roles que toman parte en él y finalmente la guía de manejo de los datos (*Data Management Body of Knowledge*) de la asociación DAMA International [8], por la que se regulan las principales dimensiones relacionadas con el tratamiento de los datos a nivel estratégico, funcional y de implementación.

La adaptación de la LOPDP en el Capítulo 4, donde se desarrolla el procedimiento y trabajo realizado, situando los distintos artículos que componen la ley orgánica en las actividades de desarrollo *software*, obteniendo así una guía comprensible que permita gestionar el cumplimiento de la normativa desde cada una de dichas fases.

En el Capítulo 5 se realiza una prueba de concepto con el análisis obtenido, para validar si la aplicación de la guía elaborada sería viable o no dentro de un proyecto de desarrollo *software* real. Para ello se utiliza el Listado de Cumplimiento Normativo de la Agencia Española de Protección de Datos.

En el Capítulo 6 se presentan las conclusiones y se trata el trabajo a futuro, donde se exponen ideas para mejorar y profundizar en el tema de la integración de la normativa al proceso de desarrollo, dando ejemplos de posibles trabajos a realizar que surgen a raíz del presente Trabajo de Fin de Grado.

Finalmente, en los Anexos se encuentra el detalle de los diferentes tipos de contextos empresariales a los que afecta la LOPDP (Anexo I), un resumen de cada uno de los diez títulos de la LOPDP (Anexo II), los artículos que se han utilizado para el desarrollo del trabajo y la actividad en la que se han tenido en cuenta (Anexo III) y el listado de todos los artículos restantes que no tienen cabida en el contexto del desarrollo *software* (Anexo IV). Finalmente, en el Anexo V se encuentra completado el cuestionario de cumplimiento del RGPD creado por la Agencia Española de Protección de Datos, aplicado dentro de la prueba de concepto.

# 2 Estado del Arte

El trabajo existente hasta el momento relacionado con el RGPD [1] o la LOPDP [2] se ha centrado principalmente en el proceso de validación de cumplimiento de la normativa una vez el sistema o aplicativo ya está en uso, desarrollando modelos que permitan automatizar dicho proceso, para que cualquier empresa, organismo e incluso persona pueda comprobar si sus sistemas o aplicaciones cumplen las normas para evitar las posibles sanciones.

Un ejemplo de mecanismo de validación es el desarrollado por el trabajo de Torre *et al.* [9], por el que mediante una serie de iteraciones se analiza cada uno de los artículos en busca de palabras clave que ayuden a identificar los distintos artefactos, junto con las relaciones entre ellos, que compondrán un modelo final que permita a una máquina entender el RGPD y así poder desarrollar, en un futuro, métodos de validación de cumplimiento automáticos, rápidos y fiables. Uno de los principales problemas a la hora de realizar el modelado surge de la dificultad de adaptar el lenguaje jurídico al lenguaje informático ya que es objeto de múltiples enfoques e interpretaciones. Además, el reglamento es genérico y pese a que también tiene en cuenta ámbitos específicos como el religioso o laboral, cada proyecto *software* es único y por lo tanto resulta complejo poder adaptar un modelado genérico a cada caso. Por otra parte, resulta complicado confeccionar una metodología de análisis que se adapte a todos los puntos variables de la normativa.

Otros enfoques plantean un acercamiento sistemático a modo de pasos como *GuideMe* de Ayala-Rivera y Pasquale [10] en el que se plantean seis etapas en las que se analiza el estado de una organización o aplicación, se planifican las acciones correctivas y se llevan a cabo para enmendar los errores de cumplimiento. El enfoque de este método es a modo correctivo, por lo que se da por hecho que el aplicativo ya existe. Por tanto, no se adapta a todo el proceso de desarrollo de *software* sino más bien al mantenimiento, en el que normalmente se realizan la mayoría de las correcciones.

Además de estos planteamientos más funcionales, existen una serie de guías para el cumplimiento desarrolladas por distintas empresas y organismos como por ejemplo la creada por la Agencia Española de Protección de Datos, que plantea una serie de indicaciones para los responsables de tratamiento [11], dándoles a conocer los derechos y deberes que tienen como responsables además de otros asuntos de interés como la metodología para realizar transferencias internacionales o el tratamiento de datos de menores. La propia Unión Europea [12] y empresas como Deloitte [4], Norton Rose Fulbright [13] y otras cuentan con sus propios *checklists* y *benchmarks* que ofrecen a sus clientes, con el objetivo de establecer una serie de pautas generales que permitan a una empresa, organismo e incluso trabajador autónomo comprobar si sus servicios, aplicaciones e infraestructuras están cumpliendo la normativa.

Dado que la mayoría de los enfoques y soluciones que se han propuesto hasta el momento se basan en la validación *a posteriori,* surge la necesidad de enfocar el problema de la falta de cumplimiento hacia la fase previa del inicio del ciclo de desarrollo. No existe ninguna guía comprensiva que permita a un equipo desarrollador conocer los principales requerimientos para que su aplicación cumpla con la normativa antes de iniciar el desarrollo. Esto facilitaría la tarea de la validación del reglamento e, incluso, la del desarrollo; ya que se reducirían notablemente los posibles errores de cumplimiento.

Mediante este Trabajo de Fin de Grado se busca abordar el problema desde el punto de vista de la validación *a priori*, buscando que el cumplimiento de la normativa sea comprensible para los profesionales del *software* y que, además, se tenga en cuenta desde el inicio del proceso de desarrollo *software* y no al final, cuando el producto ya ha sido entregado al cliente y está en su fase de mantenimiento.

# 3 Marco Teórico

A continuación, se introducen los principales conceptos básicos para tener en cuenta antes de comenzar con la adaptación de los artículos al Proceso Unificado de Desarrollo *Software* [6]. En este apartado se realizará una breve introducción al Reglamento General de Protección de Datos [1] y la Ley de Protección de Datos Personales [2], al Esquema Nacional de Seguridad [7], a los roles y actividades del Proceso Unificado de Desarrollo *Software* [6] y finalmente a la guía de manejo de los datos de la asociación DAMA International [8]. Con ello se pretende establecer una base para los conceptos de seguridad y *software* con la que realizar la adaptación de la normativa al proceso.

## 3.1 RGPD y LOPDP

El Reglamento General de Protección de Datos, en inglés *General Data Protection Regulation*, es un reglamento de carácter europeo que regula todo lo relativo a la protección de datos de carácter personal, desde el tratamiento hasta la circulación de estos. Cualquier empresa, sociedad o persona que maneje datos personales dentro de la Unión Europea o de sus ciudadanos deberá poner en práctica los deberes que se definen en ella.

Hasta el 6 de diciembre de 2018, en España estuvo en vigor la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, la cual pasó por a ser substituida por la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. Esta ley cuenta con noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales. Los diez títulos principales se presentan de forma resumida dentro del A.II. La función de esta ley orgánica no es otra que la de adaptar el RGPD al marco legislativo español, por lo que en su mayoría resulta muy semejante a éste.

El motivo de la creación del RGPD y la LOPDP surge de la complejidad que el tratamiento de los datos, y especialmente de los datos personales, tiene dada la naturaleza de estos; los datos son fluidos, están en constante transformación y crecimiento por lo que en muchas ocasiones es posible perder el control sobre ellos. Además, cuentan con un valor económico importante, sobre todo dentro del sector tecnológico. Según el artículo 4 del RGPD, se entiende por tratamiento de datos:

> *"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;"*

Dada la necesidad de regularizar el tratamiento de los datos surgen departamentos e incluso empresas dedicadas a garantizar la seguridad de los datos y su manejo para evitar que se produzcan robos o filtraciones que pongan en peligro a las organizaciones y sus usuarios y clientes.

## 3.2 Esquema Nacional de Seguridad

Antes de pasar a las fases del PUDS, es necesario introducir una serie de conceptos previos para comprender con mayor profundidad la seguridad y la importancia de ésta aplicada al manejo de datos en un proyecto *software*.

El Esquema Nacional de Seguridad [7], definido en el Real Decreto 3/2010 y en adelante ENS, tiene por objeto el establecer los principios de una política de seguridad a seguir dentro de los medios electrónicos, con la finalidad de garantizar una adecuada protección de los datos e información. Es importante destacar que pese a formar parte de un Real Decreto previo a la implantación de la LOPDP y el RGPD, se debe entender que estas últimas en ningún caso derogarán de forma automática las medidas de seguridad vigentes, por lo que el ENS todavía tiene cabida en la legislación actual.

El ENS es de obligado cumplimiento por las administraciones públicas, aunque puede servir de guía para las empresas privadas que quieran alcanzar un grado de seguridad óptimo. En muchas ocasiones los sistemas públicos y privados están bastante entrelazados entre sí, pero en ningún momento esto exime a las administraciones públicas de seguir las directrices del ENS, por lo que es necesario delimitar correctamente el ámbito público del privado.

El principio básico del ENS es la seguridad. Según se define en el capítulo II, artículo 5, la seguridad es "*un proceso integral constituido por los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema*". Es vital para no poner en riesgo la seguridad de los sistemas de información que todas aquellas personas que sean partícipes en alguna de sus fases estén previamente concienciadas de la importancia de la seguridad. El sistema de información deberá tener mecanismos que permitan prevenir, detectar y corregir los posibles fallos en la seguridad. Además, deberá ser sometido a reevaluación de forma periódica, con el fin de que las medidas tomadas no queden obsoletas.

Los requerimientos mínimos, según el capítulo III, artículo 11, que las administraciones públicas deberán cumplir para mantener la seguridad son:

- **Organización e implantación del proceso de seguridad**: Todos los miembros de la organización donde se vaya a implantar las medidas de seguridad deberán estar comprometidos con el objetivo de lograr la seguridad de los sistemas. Se delegará uno o varios responsables encargados de velar por el cumplimiento de las medidas y hacer a todos los miembros conocedores de éstas.
- **Análisis y gestión de los riesgos**: Las medidas que se adopten para mitigar los riesgos tendrán que haber sido previamente analizadas y justificadas.
- **Gestión de personal**: Todo el personal de la organización deberá contar con la formación necesaria en función de su desempeño en la misma sobre las medidas de seguridad adoptadas. Además, cada usuario deberá estar identificado en el sistema para poder llevar un registro de las actividades en el mismo.
- **Profesionalidad**: Es importante que el personal a cargo de los sistemas esté cualificado y que sea partícipe de todo el ciclo de vida del dato, desde la instalación de los sistemas de seguridad, el mantenimiento, las incidencias hasta el desmantelamiento.
- **Autorización y control de los accesos**: Se deberá controlar el acceso a los usuarios, procesos y dispositivos autorizados.

- **Protección de las instalaciones**: Es importante considerar el aspecto físico de la protección de datos ya que los datos siempre estarán en un disco físico que puede estar sujeto a manipulación, rotura e incluso robo. Como mínimo, las salas o lugares de almacenamiento deberán contar con un sistema de seguridad que evite que personas ajenas accedan a los sistemas.
- **Adquisición de productos**: En caso de contratar cualquier tipo de producto de seguridad, deberá cumplir con todos los requisitos de seguridad mencionados.
- **Seguridad por defecto**: El sistema deberá garantizar que el uso inseguro provenga de un acto consciente por parte del usuario y no por carencias de éste. Además, deberá ser sencillo y seguro de gestionar y usar.
- **Integridad y actualización del sistema**: Antes de instalar o configurar un nuevo elemento dentro del sistema deberá contar con la autorización previa, teniendo en cuenta su estado de seguridad previo con el fin de que éste no comprometa el estado del sistema. Se registrará cualquier incidente de seguridad y se llevarán a cabo los procedimientos de actuación previamente diseñados para reaccionar frente a código dañino. Con este registro se logrará avanzar en el desarrollo de la seguridad de nuestro sistema, analizando los errores previamente cometidos y creando nuevos sistemas que eviten que suceda de nuevo.
- **Continuidad de la actividad**: El sistema deberá contar con copias de seguridad para garantizar el continuo trabajo de los usuarios.
- **Mejora continua del proceso de seguridad**: Dada la naturaleza cambiante de la tecnología y por lo tanto de los riesgos que surgen de ella, es vital someter a revisión periódica las medidas de seguridad con el fin de que no queden obsoletas.

En el Esquema Nacional de Seguridad están definidas otras características como las categorías de los sistemas, las dimensiones de la seguridad y las medidas de seguridad, todas ellas definidas en los Anexos del Real Decreto 3/2010. Por tanto, la categoría de un sistema se basa en el impacto que un incidente de seguridad tendría sobre el mismo y de la repercusión sobre:

- Alcanzar los objetivos del sistema.
- Proteger los activos.
- Cumplir con las obligaciones de servicio.
- Respetar la legalidad.
- Respetar los derechos.

Para establecer la categoría del sistema se tendrán en cuenta las siguientes dimensiones (Figura 2):

- **Disponibilidad**: Se entiende por la garantía del acceso de personas, sistemas u organismos a los datos del sistema, siempre que estos estén autorizados y que puedan hacerlo de forma sencilla y segura durante el tiempo en el que el sistema esté programado para dar su servicio. Existen varias ventanas de disponibilidad estándar como 8x5, 24x7, entre otras.
- **Autenticidad**: Garantizar que aquellos usuarios autorizados que reclamen acceder a los datos sean quien dicen ser y no otro agente que esté suplantando su identidad. Existen tres métodos o categorías de autenticación: basados en algo conocido como

una contraseña, basados en algo poseído como una tarjeta de acceso y basados en una característica física como la huella dactilar o el patrón del iris.

- **Integridad**: Garantizar que los datos del sistema no han sido modificados por usuarios sin autorización previa ni por agentes externos al sistema.
- **Confidencialidad**: Garantizar que la información sólo estará disponible dentro del sistema para aquellos usuarios autorizados y no para externos. Además, se deberá garantizar que en caso de que se logre extraer información del sistema de forma ilícita, ésta no sea interpretable ni se pueda extraer datos relevantes de ella.
- **Trazabilidad**: Conocer el origen, ubicación y cambios que han afectado a un activo, además de su destino en caso de que se esté transmitiendo a otro sistema.

Como conclusión, podemos destacar que la seguridad cuenta con un factor humano destacable. Según un informe realizado por IBM en 2018 [14], un 95% de los fallos en la seguridad de las empresas e instituciones proviene a causa de un error humano. No obstante, pese a este dato es importante que los sistemas sean robustos para minimizar que existan o puedan existir errores humanos. En la Figura 3 pueden verse resumidos los principios básicos de la seguridad.

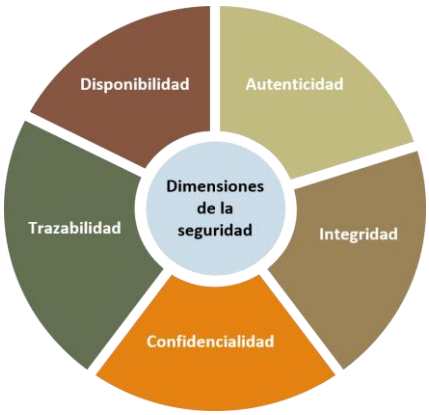


**Figura 2. Dimensiones de la seguridad**


**Figura 3. Principios básicos de la seguridad**

## 3.3 Roles y tipos de usuarios

En esta sección se definen todos aquellos roles y tipos de usuario que tomarán parte en alguna de las fases del desarrollo *software*. Dichos roles pueden ser internos o externos, y son de gran importancia dentro del proceso, ya que formarán parte de las tareas necesarias para cumplir con los requisitos del cliente y los requerimientos legales. Los roles internos serán aquellos que formen parte del equipo que va a realizar el desarrollo del producto. Los roles externos serán todos aquellos agentes partícipes del proyecto o que tengan una responsabilidad sobre él.

### 3.3.1 Principales roles internos

Están muy relacionados en su mayoría con las fases de desarrollo. Conforman el equipo encargado de ejecutar todas las etapas del ciclo de desarrollo *software*, desde el análisis hasta el mantenimiento.

- **Analista**: Persona que estudia los requisitos, especificaciones y dominio de la aplicación. Formaliza los requisitos del usuario en requisitos específicos para los diseñadores.
- **Diseñador**: Transforma el trabajo del analista en uno o varios modelos que permitan al desarrollador conocer las partes del programa y sus diferentes flujos de funcionamiento.
- **Desarrollador**: Creador del *software* mediante uno o más lenguajes de programación. En ocasiones puede ser el encargado de definir y realizar las pruebas sobre el aplicativo.
- **Personal de mantenimiento**: Encargado de realizar los cambios pertinentes una vez entregado el producto al cliente, ya sean pruebas, correcciones, mejoras del rendimiento u otras actividades.

### 3.3.2 Principales roles externos

Son todos aquellos agentes que, no siendo parte del equipo de desarrollo, toman en algún momento del ciclo de vida del *software* un papel relevante sobre alguna de las fases de éste.

- **Usuario**: a quien va dirigido el producto.
- **Cliente**: es el receptor del producto final. Puede ser también el usuario de éste.
- **Infraestructura del edificio**: lugar donde se almacenarán los datos producidos por la aplicación. Juega un rol importante ya que para cumplir ciertos grados de seguridad será necesario que cuente con distintos requerimientos.
- **Responsable o encargado del tratamiento**: determina las medidas a adoptar para garantizar que se cumpla con el reglamento de protección de datos. No es propio del PUDS, surge de la adaptación de la LOPDP.
- **Delegado de protección de datos**: delegado por el responsable del tratamiento de datos, realiza un rol semejante. No es propio del PUDS, surge de la adaptación de la LOPDP.

## 3.4 Actividades del desarrollo software

A continuación, se introduce todas las actividades del proceso de desarrollo *software* que se van a tener en cuenta a la hora de analizar la LOPDP. Dichas actividades son las descritas dentro del Proceso Unificado de Desarrollo *Software* y pueden ubicarse dentro de cuatro fases generales: inicio (definición del alcance del proyecto), elaboración (planificación), construcción y transición (entrega a los usuarios).

### 3.4.1 Captura de requisitos

En la primera actividad del desarrollo *software* el principal propósito es establecer la lista de características con las que debe contar nuestro sistema. Para registrarlas debemos concretar junto con el cliente los siguientes atributos para cada característica: nombre, descripción, estado (propuesto, aprobado, incluido, validado), coste estimado (tipo de recursos y horas-persona), prioridad (tipo de recursos y horas-persona) y nivel de riesgo asociado (crítico, significativo, ordinario).

En función de la cantidad de características y sus atributos podemos realizar una estimación del tamaño del proyecto y su duración. Dentro de los requisitos, podemos distinguir dos tipos: funcionales y no funcionales.

Los requisitos funcionales son los que podemos capturar mediante los casos de uso y representan todas aquellas funcionalidades del sistema, es decir, lo que ha de hacer el sistema. Un caso de uso, representado por un diagrama de colaboración, permite describir los actores, sistemas y acciones que participarán en cada requisito.

Los requisitos no funcionales son todos aquellos que explican cómo hace el sistema las tareas. Algunos ejemplos son la seguridad, el rendimiento o la disponibilidad del sistema. Pueden dividirse en tres tipos: requisitos del producto, requisitos organizacionales o requisitos externos [15].

### 3.4.2 Análisis

Una vez recogido todos los requisitos funcionales, deberemos analizarlos para extraer la información necesaria para diseñar nuestro sistema. El objetivo principal es estructurar y hacer más fáciles de comprender y mantener los requisitos recopilados para el equipo de diseño y desarrollo.

En la Tabla 1 podemos observar las principales diferencias entre la captura de requisitos y el análisis [6]:

| Modelo de casos de uso | Modelo de análisis |
|---|---|
| Descrito en lenguaje del cliente | Descrito en lenguaje del desarrollador |
| Vista externa del sistema | Vista interna del sistema |
| Estructurado por casos de uso | Estructurado por clases y paquetes |
| Utilizado como contrato para establecer qué deberá hacer el sistema | Utilizado para comprender cómo deberá darse forma al sistema |
| Puede contener redundancia e inconsistencias | No debe contener redundancia ni inconsistencias |
| Captura la funcionalidad del sistema | Establece cómo llevar a cabo la funcionalidad |

**Tabla 1. Diferencia entre captura de requisitos y análisis**

Aunque existen distintos métodos para realizar el análisis, la mayoría cuentan con los siguientes principios [16]:

1. Representar el dominio de la información.
2. Definir las funciones que debe realizar el software.
3. Representar el comportamiento del software en función de los estímulos externos.
4. Detallar por capas los modelos de información, función y comportamiento.
5. Llegar hasta el detalle de la implementación.

Para cumplir con estos principios es frecuente crear prototipos que sirvan como una primera aproximación del sistema a desarrollar. Estos prototipos pueden utilizarse para demostrar de forma sencilla los requisitos recogidos de la actividad anterior y, o bien se desechan al finalizar la actividad, o avanzan a las siguientes, llegando incluso a formar parte del producto final.

### 3.4.3 Diseño

Durante esta actividad se modela el sistema y su arquitectura para que sea capaz de soportar los requisitos descritos en las fases anteriores. El modelo de diseño cuenta con las siguientes características:

- Es específico para una implementación.
- Más formal que el análisis.
- Más caro de desarrollar.
- Debe ser mantenido durante todo el ciclo de vida del *software.*
- Mayor número de capas y muy centrado en la secuencia de acciones.

Dentro del diseño podemos distinguir cuatro tipos: diseño de datos, arquitectónico, de la interfaz y a nivel de componentes. En el diseño de datos se transforma en estructuras de datos aquellos dominios de información que se han recopilado en el análisis. Está muy ligado con el diseño arquitectónico, en el que se define la relación entre los elementos principales del *software*. En esta actividad se definen los patrones de diseño que se utilizarán y las restricciones de estos, además de identificar los objetos que se utilizarán en caso de ser un sistema orientado a objetos. Para esto último, es recomendable utilizar sustantivos que representen entidades tangibles, roles, eventos, localizaciones, organizaciones, etc. En esta parte del diseño, al igual que en el análisis, es común el uso de diagramas de clases, de secuencia y máquinas de estado para describir el sistema.

El diseño de la interfaz describe la forma en la que los usuarios interactuarán con el sistema y la forma de comunicarse internamente entre los módulos de éste. Finalmente, el diseño a nivel de componentes transforma los elementos de la arquitectura *software* en una descripción de los procedimientos de cada componente.

En el diseño se deberán plasmar los requisitos explícitos e implícitos del cliente en un "plano" que represente al *software* de forma abstracta en las primeras iteraciones, llegando a niveles de abstracción más bajos a medida que se avanza en el proceso. Este plano será interpretado en la implementación por los desarrolladores.

### 3.4.4 Implementación y pruebas

En la siguiente actividad se comienza a poner en práctica los resultados del diseño y se implementa el sistema, desarrollando ficheros de código fuente, *scripts*, ficheros binarios y ejecutables, entre otros.

Es en la implementación donde los desarrolladores deberán crear e integrar todos los componentes, en especial los relativos a la interfaz de usuario en caso de que el aplicativo esté orientado al uso por personas y no para ser embebido en otros sistemas. Como resultado de esta actividad se obtiene el producto, aunque no de forma final ya que deberá pasar por las pruebas e incluso se realizarán nuevas iteraciones del proceso completo.

Es en la actividad de pruebas donde comprobamos que todo lo realizado en la implementación cumple con las funciones para las que se diseñó, llevando a cabo una serie de procedimientos que nos permitan forzar el sistema para encontrar todos los fallos posibles, *bugs* o carencias de funcionalidad.

Existen varios tipos de pruebas, de las que podemos destacar las siguientes:

- **Pruebas unitarias**: aquellas en las que se prueba el correcto funcionamiento de una unidad de código, ya sea una clase, librería, método, etc. Permite comprobar que cada parte de nuestro programa funciona tal y como debe por separado.
- **Pruebas de integración**: normalmente realizadas después de las unitarias, permiten comprobar que todos los componentes del código funcionan correctamente de forma combinada. Permite encontrar fallos en dependencias o resultados no deseados.
- **Pruebas de caja negra**: comprueban que, dada una entrada, se obtiene la salida correcta sin tener en cuenta el funcionamiento interno de la clase o componente que se pruebe. Se le da importancia al qué se hace y no cómo se hace.
- **Pruebas de caja blanca**: permiten validar las funciones internas de los métodos, centrándose en cómo se hacen las operaciones y no tanto en el resultado ya que en muchas ocasiones se puede llegar a una salida correcta de forma errónea.

### 3.4.5 Mantenimiento

Una vez se han realizado todas las pruebas necesarias para considerar que el producto es estable, se entrega al cliente y da comienzo la actividad de mantenimiento. Podemos distinguir cuatro tipos de mantenimiento:

- **Adaptable**: en el que se modifica el *software* para que cumpla con nuevos requisitos.
- **Perfectivo**: en el que se mejoran los procesos existentes para aumentar su estabilidad, rapidez o seguridad, entre otros.
- **Corrective**: en el que se corrigen los errores que los usuarios, administradores u otros notifiquen.
- **Preventivo**: en el que se realizan tareas para evitar posibles problemas futuros.

Finalmente, a modo de recapitulación, se muestra en la Figura 4 el esquema de un ciclo (o "*subciclo*" en caso de ser iterativo), del proceso unificado de desarrollo *software*:

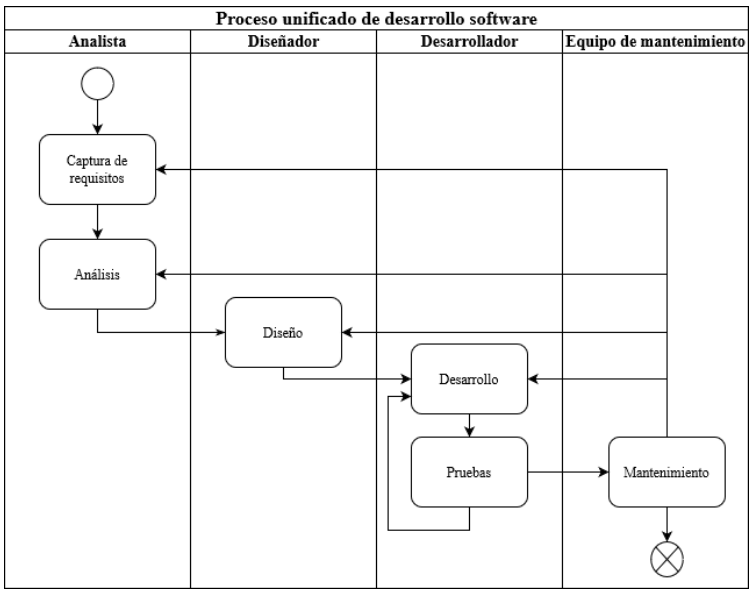


**Figura 4. Esquema de las actividades del proceso de desarrollo *software***

En un escenario real, dada la naturaleza cambiante de la tecnología e incluso del propio cliente, suele resultar difícil conseguir desarrollar cada una de las fases al cien por cien sin tener que retroceder para realizar cambios. En base a la definición de cada una de las actividades, el ciclo de desarrollo es flexible y posibilita el volver a actividades previas del ciclo, especialmente durante el mantenimiento. Con ello se consigue poder dar solución a los distintos problemas que puedan surgir a lo largo del ciclo de vida del *software*.

## 3.5 Guía de manejo de los datos

La asociación DAMA International es la asociación global encargada de la publicación de la guía de manejo de datos (*Data Management Book of Knowledge* [8]). Esta guía se ha convertido en el estándar del sector tecnológico, sentando las bases estructurales para temas como el *Big Data* o fundamentando la importancia de la calidad y ética de los datos, entre otros. En la adaptación de los requisitos tecnológicos a los requerimientos de la LOPDP se han utilizado varias de las consignas y recomendaciones que este reglamento ofrece y que se introducirán en esta sección.

La guía se divide en varios capítulos que se han relacionado con una o varias de las actividades del desarrollo *software*. Sólo se ha tenido en cuenta aquellos capítulos que tengan relación directa con el proceso de desarrollo y no con procesos puramente de gestión y organización. En el capítulo 4 se profundiza en la relación de cada capítulo con las actividades concretas. A continuación, se describe brevemente cada uno de los capítulos y la forma en la que afectan o se pueden relacionar con una o varias de las actividades del proceso de desarrollo *software*.

### 3.5.1 Gestión del Dato

La gestión del dato es el desarrollo, ejecución y supervisión de planes, políticas, programas y prácticas que permitan controlar, proteger y destacar el valor de los datos a lo largo de todo el ciclo de vida de estos. Dicha gestión va desde un enfoque más estratégico centrado en sacar el máximo valor de los datos hasta la propia implementación técnica. Es por ello por lo que podemos considerar todas las prácticas de la gestión de datos como un proceso constante que se desarrolla durante todo el ciclo de vida *software*.

Los principios de la gestión del dato se basan en lograr un balance entre las necesidades estratégicas del *software* y las necesidades operacionales, y por esta razón debemos conocer cómo son los datos que se va a tratar. Es importante reconocer que tienen un valor cualitativo y cuantitativo al tratarse de información, y por ello su valor se debe expresar en términos económicos. No obstante, difieren de los activos financieros y los activos físicos por una principal razón: no se consumen a la hora de utilizarlos por lo que su ciclo de vida es, o puede ser, bastante más duradero.

Como ya se ha mencionado, el concepto clave de la gestión del dato es el valor que tiene. Para otro tipo de activo, su valor puede calcularse de forma sencilla, por ejemplo, el valor que tiene una acción de una empresa o una flota de camiones antes de amortizarse. El cálculo del valor de los datos puede ser un proceso complicado, no obstante, podemos estandarizarlo teniendo en cuenta los siguientes elementos de cálculo:

- Coste de obtener y almacenar los datos.
- Coste de reemplazar los datos si se pierden.
- Impacto de no contar con los datos necesarios.

- Coste de mitigar riesgos potenciales.
- Coste de mejorar los datos y beneficio de los datos de mayor calidad.
- Cuánto se pagaría en el mercado por dichos datos, por cuánto podría venderse y a quién.

Una vez está claro el valor que tienen los datos dentro de nuestra organización o aplicación, podremos comenzar a planear cómo se van a gestionar. En los siguientes capítulos se detallan todas las dimensiones que hay que considerar a la hora de planificar dicha gestión, con el fin de conseguir que los datos sean veraces, actualizados, con alto valor y seguros.

### 3.5.2 Ética del Manejo del Dato

Los principios éticos sobre los datos se basan en la integridad, calidad, transparencia y confianza que una organización puede aportar a sus clientes a la hora de tratar con sus datos personales. Además, en muchos casos el tratamiento deshonesto de los datos con carácter personal es ilegal si se vulnera alguno de los derechos que se regulan por la RGPD/LOPDP; por tanto, a la hora de desarrollar una aplicación, el equipo responsable deberá tener en mente el impacto que tienen los datos sobre las personas, además de los efectos negativos sobre la economía de la organización.

En el análisis se establecerán los principios éticos por los que se regirá el desarrollo, que se deberán cumplir durante la etapa de mantenimiento con el aseguramiento de la calidad de los datos.

En el RGPD se establecen una serie de principios éticos para tener en cuenta por las organizaciones y empresas:

- Justicia y transparencia.
- Limitar el propósito de los datos personales y minimizar su uso.
- Datos exactos y actualizados.
- Garantizar la integridad y confidencialidad.
- Hacerse responsable del cumplimiento de los principios.

### 3.5.3 Gobierno del Dato

El gobierno de los datos es el ejercicio de establecer un control sobre el manejo de los datos, garantizando que se hace de forma correcta de acuerdo con las políticas y mejores prácticas establecidas, además de la ley. Se puede considerar como un proceso global que afecta a todo el ciclo de vida *software* y que se va desarrollando junto con el propio aplicativo, abarcando desde la definición de políticas de acceso, uso, seguridad y calidad hasta el propio cumplimiento de dichos requisitos. Además, a diferencia de otros, es un proceso que puede ser medido por el impacto financiero que tiene.

### 3.5.4 Arquitectura del Dato

Uno de los puntos más importantes dentro del diseño del *software* es el de la arquitectura, es decir, cómo se organizan y relacionan todos los componentes de la aplicación. El equipo de diseño deberá ser capaz de identificar los requisitos necesarios para el almacenaje y procesado de los datos para poder cumplir con los requerimientos jurídicos de la normativa.

Existen varias aproximaciones en cuanto a la arquitectura se refiere, pero pueden resumirse en los siguientes principios fundamentales:

- **Qué se va a almacenar**: todos los tipos de datos que conformen el conjunto de la información de la aplicación.
- **Cómo se va a almacenar**: todas las actividades que conformen el procesado de los datos.
- **Dónde se va a almacenar**: localización tanto tecnológica (bases de datos, almacenes de datos[1] o lagos de datos[2]) como física.
- **Quién se hará responsable**: roles que tomarán parte en el ciclo de vida del dato.
- **Cuando o cada cuanto se va a almacenar**: intervalos en los que la información se ingesta o se actualiza.
- **Por qué se almacenará**: motivos por los que se requiere guardar la información desde el punto de vista estratégico y funcional.

### 3.5.5 Modelado y Diseño del Dato

Una vez definida la arquitectura de los datos, se define cómo se van a representar los requisitos del dato. Existen varios esquemas utilizados para representar datos, entre ellos el esquema relacional, dimensional, orientado a objetos, basado en hechos, basado en el tiempo y NoSQL. El objetivo de modelar los datos es el de crear una nomenclatura estándar dentro del proyecto que permita identificar a los datos de forma sencilla para que se puedan implementar y establecer el alcance del proyecto en cuanto a la gestión de los datos.

Además de definir las propias entidades de datos, se modelan las relaciones y los atributos de éstas para obtener un mapa general de todos los tipos de datos que conformarán la aplicación.

Finalmente, a la hora de diseñar las bases de datos en las que se almacenarán estas entidades, debemos tener en cuenta los siguientes principios y buenas prácticas:

- Asegurar el **acceso fácil y rápido** a los datos.
- Permitir **reusabilidad** de las estructuras que conforman la base de datos, ya sean esquemas, tablas o columnas, entre otras.
- Garantizar la **integridad de los datos**, sin importar el contexto.
- Garantizar la **seguridad de los datos**.
- Asegurar un **mantenimiento sostenible**, es decir, que el valor de crear, almacenar, usar y desechar los datos no exceda el valor que le da la organización.

### 3.5.6 Operaciones y Almacenamiento del Dato

Una vez definida la arquitectura y el modelado de los datos, queda diseñar el apartado más técnico de ambos procesos: las bases de datos. Esta sección se centra en todas las actividades relacionadas con el ciclo de vida de los datos, desde su implementación inicial en las bases de datos hasta el proceso de eliminado de las mismas, todo ello desde el punto de vista tecnológico.

[1] Del inglés *data warehouse*, una colección de datos integrada, no volátil y variable.
[2] Del inglés *data lake*, un repositorio de datos en bruto que conserva todos los datos.

Los términos más importantes para comprender el almacenamiento del dato son los siguientes:

- **Base de datos**: colección de datos estructurada.
- **Instancia**: ejecución independiente de un *software* de control de acceso a una base de datos.
- **Esquema**: subconjunto de datos dentro de la propia base de datos o instancia, utilizado para organizar su contenido y aislarlo.

En cuanto a la arquitectura de una base de datos, existen varias formas de organizar un conjunto de bases de datos, de entre las que destacan:

- Modelo **centralizado**, en el que todos los sistemas se encuentran en un mismo lugar. Este modelo permite una gran restricción de los datos, pero una baja disponibilidad ya que si el sistema deja de funcionar no existe un sistema alternativo donde consultar los datos.
- Modelo **distribuido**, que cuenta con varios nodos por lo que permite una alta escalabilidad y disponibilidad, aunque la gestión puede resultar más compleja.
- Modelo **federado**, en el que se parte de un nodo central principal y varios nodos secundarios distribuidos, con las ventajas e inconvenientes que ambos modelos conllevan.
- Modelo ***blockchain***, basado en el modelo federado que permite manejar operaciones y transacciones financieras, entre otros tipos.
- Modelo de **virtualización** o *cloud*, en el que se descentraliza la localización de lo servidores, permitiendo unir servicios disponibles de cualquier parte del mundo para realizar las operaciones y el almacenado de los datos.

### 3.5.7 Seguridad del Dato

Uno de los temas más importantes dentro del marco legislativo es el de la seguridad de los datos personales con los que las empresas y aplicaciones tratan. La seguridad abarca todas aquellas políticas y procedimientos que se planifican en el análisis, se diseñan técnicamente durante el diseño y se ejecutan durante la implementación y el mantenimiento. Los requisitos de seguridad suelen proceder de los propios requisitos del cliente o de las directrices y regulaciones gubernamentales como es la LOPDP. Por ello, podemos distinguir entre dos tipos de restricciones: el nivel de confidencialidad, donde las organizaciones son las que deciden qué tipos de datos no deben ser conocidos por externos, y las regularizaciones, que como se ha mencionado, corresponde a todas aquellas reglas, tratados, regulaciones o leyes externas.

Los fines principales para la seguridad de los datos son permitir un acceso controlado a ellos y cumplir con las regulaciones existentes. Una mala gestión de la seguridad supone un riesgo, tanto para la empresa que gestiona los datos como para la fuente de procedencia de estos. Es por ello por lo que es necesario establecer políticas que ayuden a hacer frente a estos riesgos, sobre todo desde el punto de vista jurídico. El proceso de definición de una política de seguridad estándar sería el siguiente:

- **Definir los niveles de confidencialidad**: concretar qué tipos de datos serán confidenciales, como los personales, y cuales para uso general.

- **Definir los roles que participarán en el tratado de los datos**: partiendo normalmente desde el usuario con acceso de lectura simple hasta un administrador con poder sobre toda la organización, e incluyendo la figura del responsable de protección de datos. Normalmente los principales "poderes" que un rol puede tener son el de lectura, creación, actualización y borrado, aunque pueden existir otros.
- **Definir los procedimientos para la administración**: se deberá cumplir, como mínimo, los siguientes controles y procedimientos: cómo dar y denegar el acceso a un usuario, cómo se asigna un usuario a un rol, cómo se monitorizan los niveles de privilegios, cómo se monitorizan las peticiones de acceso, cómo se clasifican los datos en función de su grado de confidencialidad, cómo se gestionan las fisuras en la seguridad una vez detectadas.
- **Definir cómo mantener, monitorizar, auditar y cumplir con las políticas**: desde *KPIs*[3] que permitan conocer el grado de seguridad de los sistemas hasta los procesos de auditoría para asegurarse de que se cumplen con las políticas establecidas.

Finalmente, en cuanto a la implementación, existen varias técnicas y tecnologías que sirven para aplicar las políticas definidas en las fases anteriores. Algunos ejemplos, dentro del marco del desarrollo *software*, serían: uso de protocolos seguros para la transferencia de datos como HTTPS, uso de protocolos para el manejo de credenciales de los usuarios como LDAP (*Lightweight Directory Access Protocol*), establecer *firewalls* entre sistemas o partes de este para evitar tráfico de datos no autorizado o el cifrado de los datos.

### 3.5.8 Integración del Dato

A la hora de tratar con datos es muy probable que estos se deban utilizar en varios procesos o aplicaciones. Es por ello por lo que es importante conocer la ingesta, integración y transmisión de dichos datos, para poder garantizar la seguridad y eficiencia de estos procesos.

Así pues, el objetivo principal es conseguir que aquellos datos que se van a obtener o enviar estén consolidados y disponibles desde el primer momento en el que llegan a los sistemas de destino. Para ello, se desarrolla un plan de integración del dato que se definirá durante la actividad de diseño y finalmente se pondrá en práctica durante la implementación. El primer paso es conocer los posibles orígenes de los datos, para identificar aquellos que tendrán valor para la aplicación u organización. Una vez claras las fuentes, es importante documentar el linaje de dichos datos, es decir, todo lo relativo al ciclo de vida del dato, desde su origen y sus cambios hasta el momento en el que el dato se deshecha. A continuación, se estudia el perfilado de los datos, en el que se analiza la estructura de los datos, las relaciones entre ellos y las reglas de cardinalidad o valores nulos, en blanco o por defecto. Esto permitirá conocer a alto nivel el tipo de dato que se va a integrar con la aplicación a desarrollar, con lo que se podrán definir las formas en las que en la implementación se tratarán con dichos datos.

### 3.5.9 Calidad del Dato

Uno de los últimos puntos que se tratan en el DAMA-DBOK, y probablemente uno de los más importantes, es el de la calidad de los datos. Como se ha mencionado anteriormente, los datos que se utilizan en una aplicación o sistema no suelen ser estáticos dada su naturaleza

[3] *Key Performance Indicator*, medidor definido para cuantificar el nivel de rendimiento de un proceso.

cambiante. En 2017 se estimaba que cada día se generaban unos 2.500 millones de Gigabytes [17], y actualmente se cree que, en 2025, cada día se generarán tantos datos como en todo 2020 [18].

Es por ello por lo que es importante que los datos que se utilicen en una aplicación sean de calidad. Se entiende como datos de calidad aquellos que cumplan con las expectativas y necesidades de sus consumidores, es decir, se adaptan al propósito que se le pretende dar. Por ejemplo, se cuenta con datos sobre los usuarios de una aplicación y se quiere lanzar una oferta a todos aquellos que sean de sexo femenino y tengan más de 35 años, pero resulta que los datos personales que se han definido y obtenido previamente no contemplan el sexo de la persona o los datos sobre la edad se recogieron hace dos meses, pero no se han actualizado. Esto sería un ejemplo de datos de baja calidad ya que no permitirían cumplir los requisitos.

Existen dimensiones que permiten definir la calidad de los datos, aunque es posible que en función del contexto tengan aplicación real o no. Las principales dimensiones definidas para la calidad son: completitud, exactitud, consistencia, prontitud, unicidad, validez, disponibilidad y trazabilidad, aunque es posible que en función de las necesidades se definan otras.

- **La completitud** define los campos que deberán estar poblados para que se pueda dar uso a la información. Por ejemplo, se cuenta con datos sobre personas, pero el 20% de los apellidos están vacíos, por lo que la calidad no es suficiente.
- **La exactitud** asegura que los datos representan la realidad y no existen erratas.
- **La consistencia** asegura que el dato tenga coherencia dentro del sistema, es decir, si contamos con un campo *Velocidad* dentro de una tabla que define a una persona, es un campo que no tiene sentido en el contexto de la tabla.
- **La prontitud** valida que el dato esté actualizado. La unicidad, define qué campos no podrán estar repetidos para los distintos registros. Por ejemplo, el campo *DNI* está repetido para más de una persona, por lo que resulta inaceptable como información fiable.
- **La validez** consiste en que el dato sea aceptable, es decir, tenga el formato correcto.
- **La disponibilidad** asegura que el dato se pueda consultar, modificar o eliminar sin problemas cuando sea necesario.
- **La trazabilidad** consiste en asegurar que las fuentes de las que provienen los datos son fiables y reputadas y que todas las transformaciones realizadas sobre los datos han sido documentadas.

Como se ha mencionado, es posible que cada equipo de desarrollo defina sus propias métricas de calidad en función de los datos que va a utilizar en su aplicación. Por lo general, una buena métrica de calidad de los datos deberá ser mensurable, de relevancia para los consumidores de los datos, deberá definir los umbrales de aceptabilidad de esta y reflejar los posibles mecanismos de actuación en caso de no cumplir con dichos umbrales.

Además de las métricas y dimensiones existe el proceso de perfilado de datos con el que se evalúan los datos con el fin de entender los posibles desafíos en cuanto a calidad. Existen dos tipos de perfilado de datos, el orientado al metadato y el orientado al contenido. Dicho proceso sigue los siguientes pasos: identificar los metadatos, identificar las dependencias entre las tablas y finalmente identificar la redundancia.

# 4 Adaptación de la LOPDP

El siguiente capítulo sitúa cada uno de los artículos que conforman la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales [2] dentro de cada una de las actividades del PUDS [6]. Muchos de los artículos que conforman la ley son transversales a las actividades, por lo que es de esperar que estén presentes en varias de ellas. No obstante, no todos los artículos del reglamento tienen cabida dentro de alguna de las actividades dada su naturaleza puramente jurídica y que no aplica al contexto tecnológico. En caso de ser necesario por la definición del artículo, se complementa la información de éste con las referencias que contenga al RGPD [1], es decir, en varias ocasiones los artículos mencionan información crucial que se establece en el Reglamento Europeo, por lo que también se hace uso de dicha información. Todas las referencias a artículos se entenderán por artículos de la LOPDP.

A la hora de hacer la adaptación se ha analizado cada uno de los artículos que comprenden el reglamento, para determinar a qué actividad del desarrollo de *software* deben pertenecer. Para ello se han definido una serie de conceptos clave para cada una de las actividades. En función de qué conceptos aparecen en cada artículo, se han asignado a una o varias de las actividades; estos pueden encontrarse en la Tabla 2. La metodología que se ha desarrollado se resume en el siguiente flujo de trabajo (Figura 5):

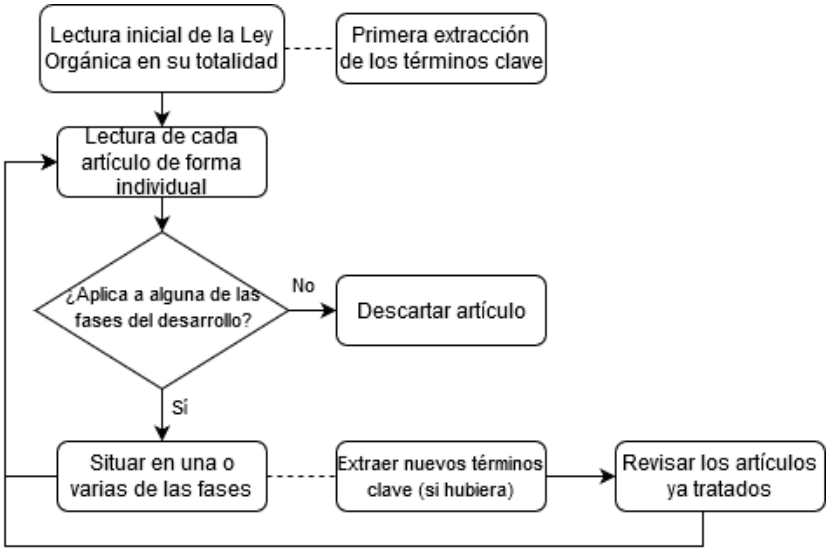


**Figura 5. Metodología desarrollada para la adaptación**

| Captura de requisitos y Análisis | Diseño | Implementación y Pruebas | Mantenimiento |
|---|---|---|---|
| Derechos y deberes | Almacenamiento | Usuario | Tiempo de vida |
| Tipos de datos | Transferencias | Validación | Ciclo de vida del dato |
| Finalidad | Arquitectura | Interfaz | Registro |
| Requerimientos | Seguridad | Consentimiento | Seguridad |
| Tratamiento | Interfaz | Comunicación / facilitar información | Control |

| | | | |
|---|---|---|---|
| Limitaciones | Comunicación / facilitar información | Derechos y deberes | |
| Evaluación | Medidas y códigos | Seguridad | |
| | Encargado del tratamiento | | |
| | Acceso a datos | | |

**Tabla 2. Terminología para la adaptación de cada artículo**

Este trabajo se ha realizado de forma manual, haciendo una primera aproximación general para cada uno de los artículos y después ajustando la localización de cada uno de ellos en función del contexto general del reglamento para obtener un hilo general que permita enlazar cada artículo. Además, se han aplicado varias de las consignas que se establecen en la normativa establecida por el DAMA [8], introducidas de forma general en el capítulo anterior. En la Tabla 3 se muestra la relación entre cada capítulo de la normativa del DAMA con la actividad correspondientes.

| DAMA | Actividad del desarrollo |
|---|---|
| **Gestión del Dato** | Análisis / Diseño / Implementación / Mantenimiento |
| **Ética del Manejo del Dato** | Análisis / Mantenimiento |
| **Gobierno del Dato** | Análisis / Diseño / Implementación / Mantenimiento |
| **Arquitectura del Dato** | Diseño |
| **Modelado y Diseño del Dato** | Diseño |
| **Operaciones y Almacenamiento del Dato** | Diseño |
| **Seguridad del Dato** | Análisis / Diseño / Implementación / Mantenimiento |
| **Integración del Dato** | Diseño / Implementación |
| **Calidad del Dato** | Diseño / Mantenimiento |

**Tabla 3. Relación entre capítulos del DAMA-DBOK y las actividades de desarrollo software**

Los procesos de gestión y gobierno del dato se consideran como globales al proceso de desarrollo ya que se tratan de actividades que se llevan a cabo durante todo el ciclo de vida del *software* dada su naturaleza funcional y de estrategia. Además, la seguridad del dato afectará también a todo el proceso ya que, de no ser así, la propia seguridad resultaría incompleta. Por ejemplo, si analizamos y diseñamos procesos de seguridad, pero no los implementamos, el trabajo sería en vano ya que las medidas en sí no existirían.

Los procesos de arquitectura, modelado, diseño, operaciones y almacenamiento pertenecen al diseño por la propia definición de la actividad, en la que se tienen en cuenta todos los requisitos relacionados con estos procesos.

La ética del manejo de los datos está estrechamente relacionada con el cumplimiento de los derechos de los usuarios, por lo que pertenecerá al análisis ya que es el paso donde se realiza

el estudio de dichos derechos y se ponen en contexto con la aplicación. Además, es un proceso que se deberá garantizar durante todo el ciclo de vida del *software*, por lo que se deberá tener en cuenta durante el mantenimiento para evitar que se incumplan las directrices planteadas en el análisis.

La integración del dato pertenece al diseño, ya que es donde se definen las formas en las que el aplicativo se comunicará entre sí, y a la implementación ya que es donde se desarrollan los mecanismos de transmisión e integración de los datos.

Finalmente, la calidad de los datos, uno de los procesos más importantes en cuanto a garantizar un correcto tratamiento de los datos, se planteará en el análisis con la definición de los tipos de datos y se llevarán las tareas propias de la validación de la calidad del dato durante el mantenimiento.

En el Anexo III pueden encontrarse las tablas con cada uno de los artículos de la LOPDP y la actividad a la que pertenecen según el análisis realizado. Además, en el Anexo IV se muestran aquellos artículos que no tienen cabida en alguna de las actividades y el motivo por el que se han descartado.

## 4.1 Captura de requisitos y análisis

A continuación, se describen todos los artículos que hay que tener en cuenta a la hora de realizar la captura de requisitos y el análisis. Se ha decidido no separar ambas actividades puesto que comparten la mayoría de los requerimientos jurídicos además de que comprenden la fase inicial de un proyecto *software*.

En la primera fase de cualquier desarrollo de *software* se deberá comenzar por la definición del alcance de los datos, es decir, qué tipos de datos se recogerán y para qué. Para ello, es importante tener en cuenta que los datos deberán ser exactos (*Art. 4*). Que un dato sea exacto significa que representa correctamente una entidad de la realidad. Por ejemplo, si se utiliza el paradigma de la orientación a objetos, a la hora de definir el objeto *Persona* se deberá concretar los atributos que necesitará la aplicación para que sean una representación real de una persona como por ejemplo el nombre y apellidos, sexo y edad, entre otros.

Si la aplicación trata con datos personales, es importante tener en cuenta si el usuario, cuyos datos personales se tratarán, aceptará dicho uso (*Art. 8*). Para ello es imprescindible que se defina el alcance del uso y la finalidad de dichos datos, teniendo en cuenta que el principal fin es buscar la satisfacción del interés de la propia persona. Para poner en contexto este requerimiento podemos tomar como ejemplo una red social. En una red social a menudo se le pide al usuario que proporcione sus datos personales como el nombre, edad, sexo, nacionalidad, además de otros aspectos más subjetivos como los gustos o las relaciones con otras personas. Por ello, debe estar bien definido el propósito de recopilar esta información, en este caso para poder identificar a personas y que se puedan establecer los vínculos sociales. Cualquier persona que acepte el uso de sus datos personales con este fin deberá ser informado de ello.

Siguiendo la línea de la definición del alcance que tendrán los datos en el proyecto *software*, es crucial poder distinguir entre los tipos de datos personales que sí se podrán usar y los que no están permitidos. Si la finalidad principal es la de identificar la ideología, afiliación sindical, religión, opiniones políticas, orientación sexual, creencias u origen racial o étnico, no se podrá hacer uso de ellos con el fin de evitar la discriminación (*Art. 9*). Tampoco se

podrán tratar datos relativos a la salud o biométricos. No obstante, existen excepciones como que el propio afectado dé su consentimiento o que el tratamiento de estos datos sea vital en un proceso jurídico (*Art. 10*). Para contextualizar, y volviendo al ejemplo del tipo de dato *Persona*, sí se podrá recoger su sexo, pero no su orientación sexual salvo que se cuente con su consentimiento explícito. En la Figura 6 se recogen de forma resumida las categorías de datos cuyo tratamiento está prohibido.

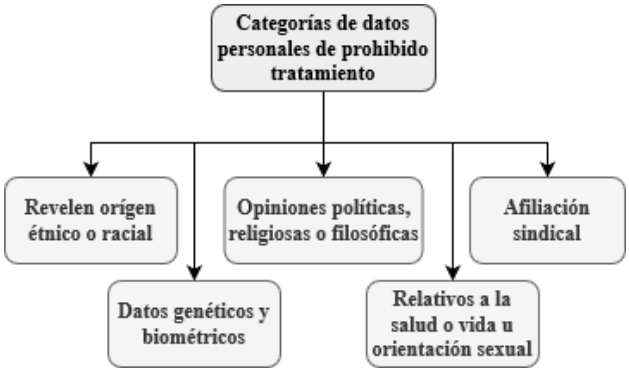


**Figura 6. Categorías de datos de prohibido tratamiento**

Así pues, por regla general, no se podrá contar con esta información en el modelo de datos salvo que ocurran alguna de las circunstancias que se mencionan en el artículo 9.2 del RGPD. Será responsabilidad del equipo de análisis el identificar si el aplicativo incurrirá en dichas circunstancias, lo que supondría que alguna de las categorías mencionadas sí podría tratarse en la aplicación.

Es importante tener en cuenta que, una vez recogidos los datos, el afectado podrá requerir que se le informe del uso que se le están dando, y más concretamente, sobre los siguientes puntos básicos: identidad del responsable del tratamiento, finalidad de este, información sobre sus derechos, que se establecen en los artículos 15 a 22 del RGPD, las categorías de datos que son objeto de tratamiento y las fuentes (*Art. 11*). Dentro del análisis inicial, y como ya se ha mencionado, es imprescindible que se establezca de forma concreta la finalidad del tratamiento con el fin de poder cumplir con este requerimiento jurídico. Según la Agencia Española de Protección de Datos [19], los tratamientos que estarán afectados por la normativa, además de los ya mencionados, son aquellos que:

- Cubran aspectos de personalidad o hábitos.
- Impliquen la toma de decisiones automatizadas.
- Monitoricen, geolocalicen o supervisen a la persona de forma sistemática y exhaustiva.
- Impliquen el uso de datos genéticos.
- Tengan por sujeto a personas vulnerables o en riesgo de exclusión social.
- Impidan al interesado ejercer sus derechos.

Por ello, si los requisitos que el cliente necesita para su aplicación implican alguno de estos tipos de tratamiento, se deberá solicitar siempre la aceptación de los usuarios. En la parte de implementación se detalla cómo solicitarla.

Dentro de los tipos de tratamientos de la lista de la Agencia Española de Protección de Datos se menciona el ejercicio de los derechos del interesado/afectado del tratamiento. Es vital que

en las primeras fases del proyecto se conozcan los derechos que los usuarios tendrán, con el fin de evitar que la aplicación no pueda cumplir con alguno de ellos. Es importante conocer además que el ejercicio de ellos puede proceder tanto del usuario en sí como de su representante legal (*Art. 12*). A continuación, se listan todos aquellos derechos con los que los usuarios contarán en cuanto al uso de sus datos personales se refiere. En la implementación se profundizará en cómo asegurar que el usuario puede hacer ejercicio de ellos (*Art. 13 a 18*).

- **Derecho de acceso**: conocer si se están tratando o no datos personales que conciernen al usuario. En caso de que el usuario haya fallecido, el derecho podrá ser ejercido por sus herederos o representantes legales (*Art. 3*).
- **Derecho de rectificación**: cambiar o completar los datos inexactos.
- **Derecho de supresión**: eliminar los datos si estos han sido tratados ilícitamente o ya no son necesarios.
- **Derecho a la limitación del tratamiento**: establecer por parte del usuario las condiciones del tratamiento.
- **Derecho a la portabilidad**: poder transmitir los datos personales a otro responsable.
- **Derecho de oposición**: evitar que los datos personales sean tratados.

Existen una serie de tratamientos concretos que se deben conocer dada la naturaleza delicada de los datos que recogen, ya que un mal tratamiento de ellos supondría un gran impacto negativo, tanto para los responsables del tratamiento como para la persona afectada. Es importante tenerlos en cuenta en función del objetivo de la aplicación *software*, como por ejemplo en el caso de aplicaciones de control bancario o de videovigilancia. A continuación, se describe brevemente cada uno de los casos.

El primero de ellos es el de los datos de contacto de empresarios individuales y profesionales liberales (*Art. 19*), relativos a una persona física que preste sus servicios en una persona jurídica. Destaca que el tratamiento sólo se referirá a los datos necesarios para la localización profesional de la persona y que el fin de este será únicamente el de mantener relaciones con la persona jurídica en la que el afectado preste sus servicios.

En el tratamiento de la información crediticia (*Art. 20*) será lícito el uso de los datos personales siempre y cuando hayan sido facilitados por el acreedor y se refieran a sus deudas ciertas, vencidas y exigibles, es decir, los datos personales de las personas morosas. Será también lícito el tratamiento cuando los datos deriven del desarrollo de una operación mercantil en la que se modifique la estructura de una sociedad, es decir, cuando una empresa adquiera, modifique o se deshaga de una de sus ramas empresariales (*Art. 21*).

En caso de que la aplicación sea de videovigilancia (*Art. 22*), sí se podrán tratar las imágenes recogidas siempre y cuando la finalidad sea la de preservar la seguridad de las personas y bienes. Es importante conocer que las imágenes se deberán destruir pasado un mes desde su captación salvo por impedimento de una acción legal.

En caso de comunicaciones publicitarias, podrán crearse sistemas de información en los que se guarden los datos de aquellos que no quieran recibir dichas comunicaciones, guardando sólo la información imprescindible para ello (*Art. 23*).

Para aquellas aplicaciones cuya finalidad sea la de establecer estadísticas, podrán tratarse los datos personales con la previa disposición de los afectados, siempre de forma voluntaria (*Art. 25*).

En el título V de la LOPDP aparecen por primera vez las figuras del responsable y el encargado del tratamiento, junto con el delegado de protección de datos (*Art 28 a 37*). El encargado del tratamiento realizará tareas en nombre del responsable, mientras que el delegado deberá ser designado por el responsable siempre que se cumpla alguno de los supuestos del artículo 37 del RGPD, y servirá de interlocutor entre el responsable o encargado y la Agencia Española de Protección de Datos y las agencias autonómicas de protección de datos. Estos tres actores se deberán tener en cuenta dentro del análisis ya que formarán parte del aplicativo como un rol con poder de decisión sobre el tratamiento de los datos.

En el artículo 28, se exponen los motivos explícitos por los que un responsable o encargado del tratamiento podrá intervenir y tomar las medidas técnicas y organizativas necesarias para garantizar que el tratamiento cumple con el reglamento. Serán los encargados de registrar todas las actividades del tratamiento. Esto podrá organizarse en torno a un conjunto estructurado de datos, es decir, podrán existir tablas donde recoger estos datos, y por ello, formarán parte de nuestro aplicativo como todos cualquier otro dato. Por esta razón, es importante conocer la existencia de este rol para adaptar las funciones de los restantes y no intervenir en los procesos de registro. Además, el responsable o encargado podrá bloquear datos (*Art. 32*), por lo que deberá tener los permisos adecuados para ello.

Uno de los aspectos más importantes que toda aplicación *software* tiene son sus usuarios y es por ello por lo que se debe conocer todos y cada uno de los derechos que estos tienen dentro del ámbito tecnológico, además de los derechos vitales ya mencionados, con el fin de que se respeten siempre durante todo el ciclo de vida de la aplicación. El primero de ellos es garantizar la neutralidad del servicio para todos los usuarios si el aplicativo está focalizado a ofrecer un servicio vía Internet (*Art. 80*).

Otro de los derechos, y quizás uno de los más importantes en cuanto al tratamiento de los datos personales se refiere, es el de la seguridad digital (*Art. 82*). Para garantizarla, durante la actividad de análisis se deberán definir los siguientes aspectos: niveles de confidencialidad de los datos, roles implicados en el tratamiento, procedimientos de administración y planes de mantenimiento, monitorización, auditoría y cumplimiento de políticas, como se menciona en el apartado 5.7 del Capítulo 3. Es de relevante importancia conocer el rango de edad de los posibles usuarios, en el caso de que sean menores, las medidas de seguridad deberán ser más estrictas en lo relativo a la difusión de imágenes o información personal de dichos usuarios (*Art. 84*). Si la aplicación está destinada para su uso en cualquier lugar donde se desarrollen actividades en las que participan menores, se deberá contar con autorización del menor y sus representantes para el tratado de los datos (*Art. 92*). Es en la toma de requisitos con el cliente donde se deberá concretar el grupo de usuarios a los que la aplicación está destinada.

Durante la toma de requisitos se define el tipo de aplicación que se va a crear para el cliente. Si se va a desarrollar una red social o un servicio equivalente en el que se cree contenido, es importante conocer el derecho a la rectificación (*Art. 85*), para que todos aquellos usuarios que difundan contenido que atente al honor, intimidad personal y derecho a la comunicación de información veraz puedan rectificar su error. Por otra parte, si el fin de la aplicación es

que se utilice en el ámbito laboral, el derecho a la intimidad aplicará a los contenidos derivados del uso de la aplicación (*Art. 87*), las grabaciones de video y sonido que se tomen en el lugar de trabajo (*Art. 89*) y cualquier sistema de geolocalización que permita localizar a los trabajadores (*Art. 90*), como por ejemplo los servicios de rastreo de paquetería. De nuevo, es crítico conocer el tipo de datos con los que se va a tratar, y se deberá considerar a estos últimos como especialmente delicados dada las serias repercusiones legales que derivarían de un mal uso o de una pérdida o robo. Además, dentro del ámbito laboral tiene especial importancia el artículo 88, por el cual se establece el derecho a la desconexión digital de los trabajadores. Fuera del tiempo de trabajo legal o convencionalmente establecido, como las vacaciones y permisos, se deberá respetar que el trabajador no esté conectado a los sistemas, herramientas o aplicaciones que la empresa ponga a su disposición para realizar su labor, aplicando también en trabajos a distancia. Durante el desarrollo se tendrán que elaborar los mecanismos que permitan limitar el uso del aplicativo para no interferir con este derecho.

Si el aplicativo cuenta con un motor de búsqueda, existe el derecho al olvido en Internet, que garantiza que cualquier usuario pueda solicitar que se elimine de los resultados todos aquellos datos que puedan estar relacionados con su nombre cuando sean inadecuados, inexactos o de baja calidad (*Art. 93*). La supresión de datos personales también aplica a redes sociales y servicios equivalentes (*Art. 94*), junto con el derecho a la portabilidad (*Art. 95*), que permite que los usuarios reciban y transmitan los contenidos que previamente habían subido a la red social.

A modo de resumen, en la Figura 7 se muestran todos los derechos que los usuarios tendrán a la hora de utilizar la aplicación que se va a desarrollar y con los que tendremos que contar para las siguientes actividades, en las que se detallará la forma en la que se deben hacer cumplir dichos derechos.


**Figura 7. Derechos fundamentales de los usuarios de una aplicación**

## 4.2 Diseño

Durante el diseño se definirá el dominio de los datos que abarcará la aplicación a raíz de los requisitos tomados y el análisis efectuado sobre estos. El deber principal a tener en cuenta para plantear los diferentes tipos de estructuras de datos, interfaces y algoritmos de la aplicación es el de la confidencialidad (*Art. 5*), por lo que se deberá garantizar que el sistema pueda proteger contra el tratamiento no autorizado, la pérdida o la destrucción de los datos personales. Además, los datos deberán ser exactos, y en caso de que sea necesario, estar actualizados (*Art. 4*). Por lo tanto, el diseñador deberá tener en cuenta cómo preparar las distintas bases de datos y qué información se volcará sobre ellas para poder cumplir con ello. Con tal fin, deberá conocer ciertas métricas sobre los datos que se almacenará, principalmente el volumen y la frecuencia con la que se actualizarán. Asimismo, las bases

de datos deberán contar con memoria suficiente, un indexado y procesamiento preciso que permita realizar consultas y generar estadísticas veraces y servicios de *backup* y balanceo que permitan acceder en todo momento a los datos.

Para diseñar un buen sistema de almacenamiento de datos es imprescindible tener en cuenta que las bases de datos no van a permanecer intactas desde su creación hasta el fin del ciclo de vida del *software*. Por ello, es una buena práctica el contar con una serie de entornos bien diferenciados:

- **Entorno de desarrollo**: en el que se probarán todos los cambios que se pasarán a producción. Suelen contar con especificaciones similares a los de producción.
- **Entorno de pruebas**: donde se realizarán pruebas de rendimiento e integración. Suelen ser iguales a los de producción en cuanto a recursos.
- **Entorno experimental**: donde se probarán nuevos planteamientos. Debe estar aislado de cualquier otro entorno.
- **Entorno de producción**: donde la aplicación estará en funcionamiento. Suelen contar con fuertes políticas de seguridad y *backup*.

A la hora de definir el modelo de datos personales, y como ya se tuvo en cuenta durante el análisis, no se podrán tratar categorías de datos que entren en conflicto con el artículo 9 y que se pueden ver resumidas en la Figura 6. A estas categorías se les añade los datos de carácter penal (*Art. 10*). Por ejemplo, si definimos un tipo de dato *Persona*, salvo por las excepciones del artículo 9.2 del RGPD, no podremos definir como atributos *Orientación sexual* o *Religión*, entre otros.

Para diseñar el modelo de datos se debe tener en cuenta las relaciones que tendrán los diferentes objetos de datos. Debido al artículo 11, por el que el afectado del tratamiento puede solicitar al responsable del tratamiento cumplir el deber de información o cualquiera de los derechos fundamentales (Figura 7), se deberá almacenar la identidad del responsable del tratamiento, la finalidad del tratamiento, las categorías de los datos objeto de tratamiento y finalmente las fuentes de las que proceden los datos, siendo esto último especialmente importante ya que afecta directamente al modelo de datos, introduciendo una relación entre los objetos de datos y la fuente de procedencia.

Además de los datos personales en sí, es decir, de los objetos de datos que se utilicen para almacenarlos, es imprescindible llevar un registro de todas las actividades de tratamiento que se efectúen sobre ellos (*Art. 31*). El registro deberá contener la siguiente información:

- Nombre y datos de contacto del responsable del tratamiento o su representante y del delegado del tratamiento, si lo hubiera.
- Finalidad del tratamiento.
- Categorías de interesados y de datos personales.
- Categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales.
- Transferencias a un tercer país u organización internacional.
- Plazos previstos para la supresión de las categorías de datos.
- Descripción de las medidas técnicas y organizativas de seguridad.

Normalmente, dicho registro tendrá una relación “N a N” entre el objeto *Registro* y los objetos afectados ya que un registro puede afectar a más de una categoría de datos y una categoría de datos puede ser tratada y registrada en más de un registro.

Es posible que en algún momento del ciclo de vida del *software* se requiera que se bloqueen alguno de los datos que se almacenan para proceder a su rectificación o eliminación (*Art. 32*); para eso se deben diseñar mecanismos que permitan identificar aquellos datos bloqueados, como por ejemplo etiquetas. Si un dato está marcado como bloqueado, no podrá ser tratado salvo por jueces o tribunales, por lo que el sistema deberá ser capaz de identificar y evitar que se estén utilizando dichos datos en alguna de las funciones del aplicativo. Un ejemplo muy común es el caso de una cuenta en una red social. Cuando el usuario solicita que se dé de baja su cuenta, el sistema bloqueará todas aquellas referencias que se hagan a dicha cuenta hasta que, finalmente, se acaba eliminando todos los datos.

En muchas ocasiones los datos no se almacenan siempre de forma estática en una misma base de datos durante todo su ciclo de vida, ya que es común que se produzcan transferencias de datos, nacionales y/o internacionales, entre distintos organismos, empresas y aplicaciones. Los responsables del tratamiento deberán informar a la Agencia Española de Protección de Datos de la transferencia, siempre que esta esté correctamente justificada (*Art. 40 a 43*). Por lo tanto, es labor de los diseñadores el preparar la forma en la que estas transferencias se llevarán a cabo, en esencia, la migración de las bases de datos a otras distintas y la forma en la que se realizará la transferencia.

Es importante tener en cuenta que existen dos tipos de transferencias internacionales: aquellas que se realicen a estados que proporcionen un nivel de protección adecuado y aquellas a estados que no lo proporcionen. En caso de ser a uno de los últimos, estarán sujetas a la autorización del director de la Agencia Española de Protección de Datos. Se entiende como transferencia o migración el proceso en el que los datos cambian de lugar de almacenamiento, sistema o formato, manteniendo siempre la misma información o contenido. Para ello se debe tener en cuenta lo siguiente [20]:

1. Establecer el alcance de la transferencia.
2. Identificar los riesgos posibles.
3. Determinar los requisitos de la migración.
4. Establecer un plan de comunicación.
5. Definir los roles y responsabilidades.
6. Determinar los controles de seguridad.

Para realizar la transferencia se llevará a cabo el siguiente proceso (Figura 8):

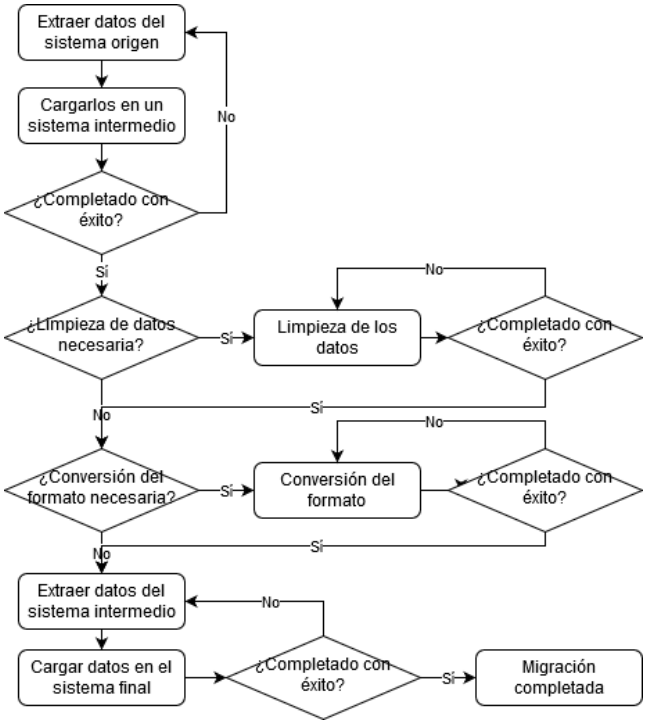


**Figura 8. Proceso de transferencia de datos entre sistemas [20]**

Como se puede observar en la Figura 8, existen dos procesos relacionados con la calidad de los datos: la limpieza y la conversión de formato. Los planes de evaluación de la calidad en las transferencias de datos se desarrollarán durante la implementación de la transferencia, pero se deberán definir en el diseño del modelo de datos y metadatos. Por ejemplo, si contamos con un campo *Teléfono* que previamente se ha definido como numérico y durante la transferencia se observa que aparecen letras, sería una incidencia que requeriría de limpieza. Este tipo de errores pueden definirse previamente realizando el perfilado de los datos como se menciona en el apartado 5.9 del Capítulo 3.

Finalmente, tanto en las transferencias de datos como en el propio almacenado y tratamiento de los datos, se debe garantizar la seguridad de estos procesos (*Art. 82*). Siguiendo las directrices determinadas en el apartado 5.7 del Capítulo 3, en el diseño se deberán plasmar de forma más técnica los requisitos de seguridad, estableciendo con los diagramas de interfaz la forma en la que los módulos de la aplicación se conectarán entre ellos y con el exterior, con las matrices RASCI[4] los niveles de responsabilidad y con las políticas de administración todos los aspectos relevantes de gestión de la seguridad. Estas medidas se codificarán y pondrán realmente en práctica durante las actividades de implementación y pruebas y el mantenimiento.

## 4.3 Implementación y pruebas

En la siguiente fase se traduce el diseño en código y se realizan las pruebas necesarias para confirmar que la implementación es correcta. Un buen análisis y diseño permitirá que esta fase sea, probablemente, la más sencilla en cuanto a los requerimientos jurídicos. Durante la implementación se desarrollará principalmente la forma en la que se hará conocedor al usuario de todos los derechos con los que cuenta y cómo se recogerá el consentimiento al tratamiento de los datos personales.

[4] De las siglas en inglés *Responsible, Accountable, Support, Consulted* e *Informed*

A la hora de desarrollar la aplicación se debe tener en cuenta que se dará como válida la conformidad del tratamiento de los datos cuando la persona manifieste de forma voluntaria, específica, informada e inequívoca, la conformidad mediante una clara acción afirmativa (*Art. 6*). Es por ello por lo que será necesario incorporar alguna vía por la que el usuario pueda confirmar el tratamiento de sus datos. Un ejemplo sería una ventana emergente que le informase de ello, y que permita aceptar o rechazar el almacenamiento y uso de los datos. Es importante mencionar que en ningún caso se podrá marcar como aceptado el consentimiento previa aceptación del usuario. Es decir, en caso de que contemos con un *checkbox* en el que se solicite el consentimiento del tratamiento de los datos, en ninguna circunstancia podrá estar marcado por defecto. Además, será necesario contemplar una forma con la que poder informar al usuario del tratamiento que tendrán sus datos y otro tipo de información jurídica que pueda influir en la decisión de aceptar o no. Para los datos de geolocalización (*Art. 90*), es común el uso de ventanas emergentes en las que se solicite si el usuario acepta que se active la localización de su dispositivo, con el fin de dar una mejor experiencia y aumentar cierta funcionalidad del aplicativo.

Cabe resaltar que el consentimiento anterior a la entrada en vigor de la normativa no tiene por qué volver a solicitarse y que el consentimiento puede ser parcial o total. Además, existen otros métodos con los que solicitarlo como la integración de la firma virtual o la validación por certificados proporcionados por entidades como autoridades de certificación como pueden ser la Fábrica Nacional de la Moneda y Timbre, que expide certificados digitales de persona física que permiten identificarse en Internet.

Como se menciona en el análisis, será necesario validar la mayoría de edad del usuario (*Art. 7*). El tratamiento de los datos de un menor de catorce años solo será lícito si se cuenta con el consentimiento de sus tutores legales, por lo que será necesario recoger de alguna forma dicho consentimiento. Una de las principales formas es mediante un *pop-up* o un formulario a cumplimentar por el tutor, aunque existen otras formas válidas como pedir que dicha información se envíe directamente a la empresa por parte del usuario. Es posible que, en caso de no contar con dicho consentimiento, sea necesario restringir el uso de la aplicación, como, por ejemplo, eliminando las funciones *online* de la misma o que el usuario menor de edad pueda subir contenido a ella. De alguna forma, se asemeja a aceptar el uso de *cookies* ya que le estamos dando permiso a la aplicación de que registre nuestros datos y en muchas ocasiones el no hacerlo restringe el uso de la aplicación.

En cualquier momento el usuario de la aplicación podrá solicitar el acceso a los datos que haya proporcionado junto con el cumplimiento de todos los derechos que se recogen en los artículos 13 a 18 y 80 a 96, por lo que se deberá contemplar una forma para que se pueda realizar dicha solicitud y cumplir con el deber de información. Según el artículo 11, se podrá indicar una dirección electrónica u otro medio para que pueda acceder a la información, conteniendo esta misma la identidad del responsable del tratamiento, la finalidad de este y la posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del RGPD junto con la información básica y las fuentes de procedencia de los datos.

Para el artículo 88 en especial, se tendrán que contemplar medidas para garantizar la desconexión digital y evitar la fatiga informática como por ejemplo limitar las comunicaciones al horario establecido o recordar cada cierto periodo que es recomendable realizar una breve pausa para evitar dicha fatiga. Normalmente este tipo de medidas no son bloqueantes en su totalidad, es decir, si por ejemplo se establece un horario en el que no se

pueden enviar correos electrónicos, el aplicativo informará de esta norma, pero permitirá su envío ya que puede tratarse de una situación de emergencia o alta importancia.

A modo de recapitulación, y como regla general, se deberá incluir un aviso legal en el producto en el que se informe del propietario del aplicativo o página web, de la política de privacidad en la que se informe del tratamiento, su propósito, si tiene destinatarios y cuáles son, la identidad y dirección del responsable del tratamiento y finalmente informar de los derechos del usuario. También será necesario incluir la política de cookies en caso de que se utilicen, indicando cuáles se utilizan, con que finalidad y durante cuánto tiempo.

## 4.4 Mantenimiento

Cuando el producto ya ha sido entregado al cliente, una vez haya completado la actividad de pruebas, pasará al mantenimiento. Normalmente el encargado de mantenimiento es el equipo desarrollador, aunque en algunos casos puede delegarse a un equipo especializado en el mantenimiento. En esta actividad se aplicarán la mayoría de las directrices relacionadas con la seguridad y la calidad de los datos.

Durante el tiempo de vida del producto es posible que muchos de los datos que se han recogido vayan cambiando o desapareciendo, siendo incluso posible que alguna de las personas de las que han recopilado datos fallezca. Debido a ello, sólo las personas vinculadas a un fallecido por razones familiares o por ser herederos podrán solicitar el acceso a los datos de dicha persona si no hubiera sido prohibido explícitamente por la misma (*Art. 3*). Dichas personas podrán decidir si se modifican o se eliminan los datos del fallecido. La figura del responsable de datos participará en caso de que sea necesario bloquear los datos (*Art. 32*). Para ello deberá identificar y prevenir que sean visualizados por cualquier persona u organismo a excepción de jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes. En caso de que no se produzca el desbloqueo, finalmente deberá destruir los datos. Además, dicho responsable será el encargado de registrar todas aquellas actividades que se produzcan sobre los datos (*Art. 31*), con el fin de mantener un seguimiento fiable de que los datos son correctamente tratados en el caso de que se solicite dicha información.

Una de las consignas más importantes de la calidad de los datos es su exactitud. Según el artículo 5, los datos serán exactos y si fuera necesario, actualizados. Es durante el mantenimiento del producto *software* cuando los encargados de éste deberán realizar tareas para validar dichas premisas. Tampoco podrán mantenerse durante más tiempo del necesario para el tratamiento. Existen varias técnicas para garantizar la exactitud y actualidad de los datos, como validar con el propio usuario si sus datos son correctos cada cierto tiempo o realizar escáneres de las bases de datos en busca de campos inválidos, incompletos o vacíos.

En este punto del proyecto, es importante conocer que existen métodos de certificación por los que validar que el producto final cumple con los estándares y directrices que se han tratado a lo largo de este trabajo (*Art. 39*). Cabe destacar que la certificación será voluntaria y su proceso de obtención será transparente, además de que no limitará ni librará al responsable del tratamiento de la aplicación del reglamento. La duración máxima de la certificación será de tres años y en España podrá ser llevada a cabo por la Entidad Nacional de Acreditación, que informará a la Agencia Española de Protección de Datos del proceso. Con dicha acreditación podremos validar que todos los procedimientos, planes, diseños e implementaciones que se han llevado a cabo durante toda la fase de desarrollo del proyecto *software* cumplen con las directrices marcadas por el RGPD y en especial con la LOPDP.

# 5 Prueba de Concepto

En el siguiente capítulo, se realiza una prueba de concepto sobre el desarrollo de un ejemplo de aplicación *software*, que en este caso es una red social semejante a Facebook, ya que se ha considerado como el mejor ejemplo de caso de uso para la aplicación de requerimientos de protección de datos personales dentro del marco tecnológico.

El objetivo principal es, desde el punto de vista del equipo de desarrollo, validar que las directrices que se han indicado en el capítulo anterior para cumplir con la LOPDP [2] resultan posibles de llevar a cabo en un proyecto real. La prueba de concepto se dividirá en las distintas actividades del PUDS [6] que se han tomado para la elaboración de la adaptación, siendo estas la toma de requisitos y análisis, el diseño, la implementación y pruebas y por último el mantenimiento.

Para validar que la supuesta aplicación cumple con las directrices de la ley, se utilizará el Listado de Cumplimiento Normativo de la Agencia Española de Protección de Datos [21], que, pese a que se centra en el cumplimiento del RGPD [1], permite realizar una valoración aproximada al cumplimiento de la LOPDP dada su similitud.

## 5.1 Captura de requisitos y análisis

El proyecto comenzará por la delimitación del alcance de los datos. Al ser una red social, se contará con el objeto *Persona*. El propósito de recoger estos datos será el de identificar el usuario para que otros puedan conectar con él. Además del objeto *Persona*, será necesario contemplar la figura del *responsable del tratamiento*, de la que se almacenará su identidad, y un registro de las actividades del tratamiento, por lo que existirá el objeto *Registro*. El responsable tendrá el permiso de bloquear datos. Por último, existirá el objeto *Administrador*, que será el responsable de la gestión del sistema y sus usuarios.

Dado que es una red social en la que los usuarios podrán expresar sus opiniones, se cubre el aspecto del tratamiento de datos sobre personalidad, por lo que habrá que solicitar la aceptación al usuario sobre dicho punto. Los usuarios podrán editar el contenido que hayan creado, y si deciden eliminar su perfil, dejarán de aparecer en los resultados de búsqueda dentro del aplicativo. Cualquier contenido que creen podrá ser exportado fuera de la aplicación.

El modelo de negocio se basará en la muestra de publicidad dentro de la aplicación y la venta de los datos a terceros, por lo que se podrá crear un sistema de información donde guardar la información de aquellos usuarios que soliciten no recibir dicha publicidad. Además, al tratarse de un servicio en Internet, deberá ser neutral, es decir, que cualquier usuario contará con el mismo servicio sin distinguir su condición. También se producirán ventas de datos a terceros, por lo que se deberá contemplar los procesos de transferencia de datos entre sistemas.

Para garantizar la seguridad digital se establece lo siguiente: implicación del *responsable del tratamiento,* nivel de confidencialidad alto para los datos de las personas, dado que se almacena información que permite identificar a un individuo, y registro de actividades. La red social será sólo accesible para mayores de dieciocho años, por lo que no será necesario contemplar los aspectos del tratamiento de datos de menores.

## 5.2 Diseño

Dentro del objeto *Persona* definiremos como atributos *Nombre completo*, *Edad* y *Sexo*. Dichos datos no entran en ninguna de las categorías que se marcan en la Figura 6, por lo que el consentimiento explícito no será necesario. El *Registro* contará con los atributos que se mencionan en el apartado 2 del Capítulo 4 y se relacionará con el *responsable del tratamiento* y la *Persona.* Cada *Persona* tendrá una relación N a N entre ella. Cada objeto contará con una etiqueta que indicará si el dato está bloqueado o no. En caso afirmativo, no se mostrará en la aplicación a ningún usuario.

Además, se guardará en el *Registro* la procedencia de los datos de las personas, que en este caso será del propio usuario cuando dio su consentimiento al registrarse en la aplicación.

## 5.3 Implementación y pruebas

Al registrarse, se informará al usuario mediante una ventana emergente de que la aplicación almacenará sus datos y de la aparición de anuncios dentro de la aplicación. El usuario deberá pulsa sobre un botón de "Confirmar" para poder registrarse en la aplicación. Al ser disponible sólo para mayores de dieciocho años, se le exigirá su edad como requisito imprescindible para registrarse.

Dentro de la aplicación aparecerá un apartado donde se recogerán todos los derechos que aparecen en la Figura 7. Además, se incluirá un apartado con el aviso legal, la política de privacidad establecida, la identidad del responsable del tratamiento y un botón donde, al pulsarlo, llevará al usuario a un sistema de solicitud para pedir el acceso a los datos personales que se hayan almacenado en la aplicación.

## 5.4 Mantenimiento

Cualquier usuario podrá solicitar la retirada de los datos de una persona fallecida, para lo cual se dará la opción de hacerlo sin necesidad de registrarse. Además, se realizarán comprobaciones de la exactitud y actualidad de los datos. En caso de que se identifique algún dato no exacto o actualizado, se informará con un mensaje al usuario para que lo complete o actualice.

## 5.5 Aplicación del listado de cumplimiento

Una vez creada la prueba de concepto se realiza una prueba de cumplimiento siguiendo los requerimientos establecidos por el Listado de Cumplimiento Normativo de la Agencia Española de Protección de Datos [21]; por cada uno de los doscientos sesenta y siete requerimientos se indica si el trabajo de adaptación del Capítulo 4 y prueba de concepto cumple con él, si no aplica al contexto del desarrollo *software* o si no se ha tenido en cuenta a lo largo de la adaptación. En el Anexo V se encuentra el listado completo con la indicación sobre el cumplimiento.

El procedimiento realizado ha sido el siguiente: por cada requerimiento del listado se analiza si en la adaptación de la normativa, bien sea por la aplicación directa de alguno de los artículos o por requerimientos derivados, se ha tenido en cuenta y si un equipo de desarrollo que utilice dicha adaptación podrá aplicarlo directamente. Por ejemplo, para el requerimiento *"Se recogen los datos personales con fines determinados",* en el apartado 1 del Capítulo 4 se indica que *"... es imprescindible que se defina el alcance del uso y la finalidad de dichos datos ..."* por lo que en la adaptación sí se ha tenido en cuenta. Gracias a ello, en la aplicación

que se plantea en este apartado se tiene en cuenta y cumple con los requerimientos de la normativa. No obstante, la adaptación del Capítulo 4 no tiene en cuenta ciertos aspectos que sí aparecen en el formulario de cumplimiento como, por ejemplo, *"Se pueden demostrar que los datos anonimizados no permiten identificar a los interesados"*, ya que en la adaptación no se ha entrado en detalle en la forma de anonimizar por lo que, a la hora de desarrollar la aplicación, podría ocasionar una falta de cumplimiento.

Finalmente, existen principios como *"Se facilita verbalmente (la información relativa al tratamiento), previa acreditación de la identidad del interesado"* que no tienen lugar dentro del contexto tecnológico ya que no tienen relación con ningún proceso que implique al *software*.

El resultado obtenido ha sido que, de los doscientos sesenta y siete requerimientos, ciento veintiocho sí se cumplen, setenta y nueve no aplican y sesenta no cumplen con la normativa. En la Figura 9 puede observarse dicho resultado.

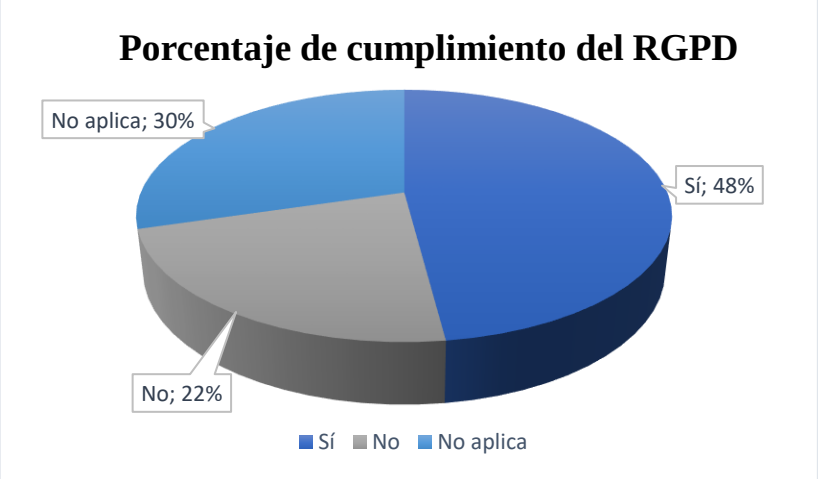


**Figura 9. Porcentaje de cumplimiento del RGPD**

Por lo tanto, dado que el 30% de los requerimientos no se considera que sean aplicables al PUDS, podemos considerar que obtendríamos un 78% de cumplimiento sobre el total de los requerimientos en caso de cumplir el porcentaje no aplicable.

Si contemplamos únicamente el porcentaje de requerimientos aplicables al marco tecnológico, es decir ciento ochenta y ocho eliminando los no aplicables, estaríamos obteniendo aproximadamente un 68% del cumplimiento. Pese a ser un porcentaje alto, queda en evidencia que aproximadamente un 30% de los requerimientos del RGPD que implican un aspecto técnico o relacionado con el PUDS no se cumplirían únicamente con las medidas *a priori* que se han establecido.

# 6 Conclusiones y Trabajo Futuro

## 6.1 Conclusiones

En el presente Trabajo de Fin de Grado se ha analizado la LOPDP [2] y se concluye que ofrece una forma de garantizar un tratamiento honesto, transparente y seguro de los datos personales para todas aquellas empresas españolas o que trabajen con datos de ciudadanos españoles. Por este motivo, resulta evidente que aplicar la normativa dentro del entorno tecnológico es de vital importancia, sobre todo para el equipo de desarrollo *software* al que va destinado este trabajo.

En una primera instancia se pretendió situar cada uno de los artículos, además de en una o varias actividades de desarrollo, en un contexto empresarial como los que se mencionan en el Anexo I, pero se comprobó que tal diferenciación no tenía sentido dado el carácter generalista de la normativa, por lo que hubiera resultado una tarea sumamente complicada y que no aportaría información vital en el marco del proceso unificado de desarrollo.

La tarea que ha resultado más compleja ha sido la del estudio, análisis y situación de cada uno de los artículos ya que, pese a contar con el conocimiento necesario sobre el ámbito tecnológico, los textos jurídicos pueden ser de gran complejidad para alguien con nulo conocimiento sobre la materia. No obstante, una vez situados, ha sido sencillo proponer las posibles soluciones para cada uno de los requerimientos al haber seguido un estándar como el de la asociación DAMA International [8].

Cabe destacar que, al ser una tarea manual, es sujeto de múltiples interpretaciones por lo que cualquier otra forma de situar los artículos dentro de las actividades del desarrollo puede resultar válida con su conveniente justificación. Aun así, la tarea de análisis de cada uno de los requerimientos sí es general ya que surge de necesidades técnicas, cuyas soluciones, normalmente ya estipuladas, probadas y validadas por la comunidad de desarrolladores.

Por último, como puede comprobarse por la prueba de concepto, la variable de la interpretación del texto jurídico juega un papel muy importante. Con el análisis realizado se ha obtenido un 68% del cumplimiento marcado *a posteriori*, y, pese a ser cumplimiento del RGPD, podemos tomar como válido dicho porcentaje dada la gran similitud entre el RGPD y la LOPDP. Así pues, el análisis desde el punto de vista puramente técnico resulta incompleto, por lo que se ha llegado a la conclusión de que sería necesario añadir una figura con conocimiento jurídico al análisis, para poder tener en cuenta todos aquellos matices jurídicos que se han podido perder durante el estudio de la ley. También resultaría imprescindible profundizar en algunos de los detalles de ciertos artículos, ya que se propone una implementación general que puede resultar incompleta. Un ejemplo de ello sería los tipos de tratamiento con fines de investigación científica, históricos o médicos, que pueden tener especial relevancia en algunos proyectos *software*.

## 6.2 Trabajo Futuro

Este proyecto puede continuar si se enfoca en el marco del reglamento europeo, realizando el mismo ejercicio de situar cada uno de los artículos del RGPD [1] utilizando la misma metodología de análisis. Además, se puede analizar otros reglamentos vigentes que resulten de especial relevancia como el de los Estados Unidos de América, cuya particularidad radica

en el hecho de que, a diferencia de Europa, la competencia legislativa recae sobre cada uno de los estados y no sobre una entidad única como es el Parlamento Europeo.

Otra sugerencia de trabajo a futuro es integrar cada una de las normativas de los principales países y organismos en un reglamento universal, facilitando a los desarrolladores una forma de garantizar una base sólida para el correcto tratamiento de los datos personales en las aplicaciones y sistemas, permitiendo ser completado con los requerimientos de las normativas nacionales o estatales para que el cumplimiento sea total.

Dado que el presente trabajo se ha centrado en el Proceso Unificado de Desarrollo *Software* [6], sería interesante realizar la misma aproximación para otro tipo de metodologías como SCRUM, Kanban o modelo en cascada. Para ello, se analizaría cada una ellas para identificar las diferentes fases que se proponen y, en función de los requisitos de cada fase, aplicar sobre ellas el algoritmo desarrollado para el PUDS con el que realizar la clasificación de los artículos. Dado que el presente trabajo se ha centrado en el ciclo de vida técnico del *software* y no en procesos de gestión, podría centrarse en éstos últimos de la misma forma.

Para finalizar, la metodología desarrollada en este trabajo podría servir de base para crear un proceso automático que permita analizar cada uno de los reglamentos vigentes y adecuarlo al PUDS. Dados una serie de parámetros como las palabras clave, y utilizando técnicas de procesamiento del lenguaje natural, se debería elaborar una tabla de equivalencias entre términos jurídicos y técnicos que permita realizar el análisis. Se pueden desarrollar algoritmos de aprendizaje automático que aprendan de la equivalencia establecida entre el contexto jurídico y tecnológico y permitan realizar el análisis y clasificación de las normativas de forma más rápida, segura y escalable, por ejemplo a todo el entorno de la Unión Europea u otros países.

# Referencias


[1] Parlamento Europeo y Consejo, *Reglamento General de Protección de Datos (UE) 2016/679*, 2016.

[2] BOE - Jefatura del Estado, *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*, 2018.

[3] PricewaterhouseCoopers US, «GDPR Compliance Top Data Protection Priority for 92% od US Organizations in 2017,» 23 enero 2017. [En línea]. Available: https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html. [Último acceso: 7 abril 2020].

[4] Deloitte, «The Deloitte General Data Protection Regulation Benchmarking Survey,» noviembre 2017. [En línea]. Available: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-nwe-gdpr-benchmarking-survey-november-2017.pdf. [Último acceso: 7 abril 2020].

[5] GDPR EU, «How the GDPR could change in 2020,» 2019. [En línea]. Available: https://gdpr.eu/gdpr-in-2020/. [Último acceso: 6 abril 2020].

[6] G. B. J. R. Ivar Jacobson, El Proceso Unificado de Desarrollo de Software, Addison-Wesley, 2001.

[7] BOE - Ministerio de la Presidencia, *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica*, 2010.

[8] DAMA International, The DAMA Guide to The Data Management Body of Knowledge, Technics Publications, 2017.

[9] G. S. M. S. L. C. B. Damiano Torre, «Using Models to Enable Compliance Checking against the GDPR: An Experience Report,» IEEE, Múnich, Alemania, 2019.

[10] L. P. Vanessa Ayala-Rivera, «"The Grace Period Has Ended": An Approach to Operationalize GDPR Requirements,» IEEE, Dublín, Irlanda, 2018.

[11] Agencia Española de Protección de Datos, «Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento,» 2019.

[12] GDPR Unión Europea, «GDPR checklist for data controllers,» [En línea]. Available: https://gdpr.eu/checklist/. [Último acceso: 7 abril 2020].

[13] Norton Rose Fulbright, «GDPR Checklist,» abril 2018. [En línea]. Available: https://www.nortonrosefulbright.com/en/knowledge/publications/3b14a527/gdpr-checklist. [Último acceso: 7 abril 2020].

[14] IBM, «X-Force Threat Intelligence Index,» 2018. [En línea]. Available: https://www.ibm.com/downloads/cas/MKJOL3DG. [Último acceso: 29 marzo 2020].

[15] I. Sommerville, Software Engineering, Boston: Pearson Education, 2011.

[16] R. Pressman, Ingeniería del Software. Un enfoque práctico, Boston: McGraw-Hill Education, 2002.

[17] Europapress, «https://www.europapress.es/portaltic/internet/noticia-cada-dia-generan-2500-millones-gb-datos-ibm-crea-plataforma-empresas-aprovechen-20170323162319.html,» *Europapress*, 23 03 2017.

[18] Orange España, «¿Cuánta información se genera al año en el mundo?,» 30 abril 2019. [En línea]. Available: http://blog.orange.es/red/datos-mundo/. [Último acceso: 06 mayo 2020].

[19] Agencia Española de Protección de Datos, «Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4)».

[20] U.S Department of Education, «Data Migration Roadmap,» 2019. [En línea]. Available: https://studentaid.gov/sites/default/files/fsawg/static/gw/docs/ciolibrary/Data_Migration_Roadmap_Guidance.pdf. [Último acceso: 10 marzo 2020].

[21] Agencia Española de Protección de Datos, «Listado de Cumplimiento Normativo».

[22] Real Academia Española, «Diccionario de la lengua española, 23.ª edición,» [En línea]. Available: https://dle.rae.es. [Último acceso: 1 Junio 2020].

# Glosario

| | |
|---|---|
| DAMA-DBOK | DAMA International *Data Management Book of Knowledge* |
| *Data Lake* | Repositorio de datos en bruto que conserva todos los datos sin jerarquía entre ellos. Permite la centralización de fuentes para ser analizadas por procesos *big data*. |
| *Data Warehouse* | Colección de datos integrada, orientada a un ámbito específico y variable en el tiempo. Permite registrar los datos de una organización y facilita el análisis de ellos. |
| EMEA | *Europe, Middle East and Africa* |
| ENS | Esquema Nacional de Seguridad |
| HTTPS | *Hypertext Transfer Protocol Secure* |
| KPI | *Key Performance Indicator* – Indicadores que permiten medir el progreso hacia una meta de forma objetiva, ofreciendo una forma de comparar el desempeño a lo largo del tiempo |
| Kanban | Método para la organización y gestión de proyectos ágiles, basada en un tablero dividido en fases, donde se apuntan las tareas necesarias a realizar |
| LDAP | *Lightweight Directory Access Protocol* |
| LOPDP | Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales |
| Matriz RASCI | Del inglés *Responsible, Accountable, Support, Consulted, Informed* – Matriz de asignación de responsabilidades utilizada en la gestión de proyectos para delimitar el rango de acción de un rol o usuario |
| PUDS | Proceso Unificado de Desarrollo *Software* |
| Requerimiento | Acto judicial por el que se intima que se haga o se deje de ejecutar algo [22] |
| Requisito | Circunstancia o condición necesaria para algo. [22] |
| RGPD | Reglamento General de Protección de Datos |
| SCRUM | Metodología de trabajo ágil utilizada para el desarrollo *software*, basada en ciclos cortos o *sprints* en los que realizar las tareas |

# Anexos

## I. Contexto empresarial

A continuación, se introducen los principales contextos empresariales en los que se aplica la Ley de Protección de Datos. Este contexto es importante a la hora de definir el grado de afección de cada artículo, el cual variará en función del tipo de empresa que se trate. Además, la forma en la que las leyes afectan puede variar en función del tipo de trabajo a realizar por la empresa o el trabajador. Por ejemplo, una empresa relacionada con la sanidad debe controlar sus datos de forma distinta a cómo debe hacerlo una empresa de telecomunicaciones.

Se distinguen cuatro tipos de contextos, el de un trabajador autónomo, el de la pequeña, mediana o gran empresa y finalmente el de la administración pública. A continuación, se describe cada tipo de contexto.

**Trabajador autónomo**
Dícese de la persona que trabaja por cuenta propia. Es una persona física que realiza trabajos sin estar ligado por un contrato laboral a una empresa o la administración pública. Responde por su cuenta de las actividades de su trabajo con todos sus bienes, presentes y futuros.

El grado en el que la Ley de Protección de Datos afectará a una persona autónoma es notablemente menor que al de una gran empresa, aunque dependerá también del tipo de trabajo que desempeñe (véase cualquier profesional del ámbito médico).

**Pequeña y mediana empresa**
Se entiende por mediana empresa aquella que cuenta con menos de 250 efectivos, un volumen de negocio no superior a los a los 50 millones de euros y un balance general no mayor a los 43 millones de euros.

Una pequeña empresa es aquella que cuenta con menos de 50 efectivos, volumen de negocio no superior a los 10 millones de euros y un balance no mayor de 10 millones de euros.

**Gran empresa**
Gran empresa es toda aquella que exceda los 250 efectivos, volumen de negocio superior a los 50 millones de euros y un balance general mayor de 43 millones de euros.

A diferencia de las pequeñas y medianas empresas, suelen contar con más medios y, por ende, muchas de las leyes aplicarán de forma distinta.

**Administración pública**
Conjunto de organizaciones públicas que realizan la función administrativa y de gestión del Estado. Relaciona el poder político con la ciudadanía. Formalmente se puede entender como los organismos públicos con poder político para atender a las necesidades de la ciudadanía. Materialmente se refiere a la actividad administrativa, la gestión y la satisfacción de las necesidades públicas.

## II. Resumen por capítulo de la Ley Orgánica 3/2018

A continuación, se presenta de forma resumida cada uno de los títulos que componen la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales [2].

**Título I**

En este título se pretende adaptar el ordenamiento jurídico español al reglamento de la Unión Europea. En él se establece el derecho fundamental de las personas físicas a la protección de datos personales. Cada comunidad autónoma contará con las competencias necesarias para ejecutar dicho derecho.

Regula lo relativo a los datos de personas fallecidas, permitiendo que aquellas personas vinculadas al fallecido sean familiares o herederos, puedan solicitar el acceso a dichos datos rectificándolos o suprimiéndolos si fuera necesario.

**Título II**

Este título establece que no será imputable la falta de exactitud de los datos recogidos al responsable del tratamiento siempre que este haya adoptado las medidas necesarias para que puedan ser suprimidos o modificados.

También se recoge el deber de confidencialidad en el tratamiento de datos. En consentimiento del uso de los datos personales deberá ser claro y afirmativo por parte del afectado, sin contemplar ya el consentimiento tácito. Es a partir de los catorce años la edad en la que un menor puede dar su consentimiento sobre sus datos personales.

Se prohibirá almacenar datos con la finalidad de establecer listados identificativos como por ejemplo “listas negras” de sindicalistas.

**Título III**

Este título es una adaptación al Derecho español de los principios de transparencia en el tratamiento de datos personales en el reglamento europeo. En él, se regula el derecho a ser informado respecto al tratamiento de datos y recoge la “información por capas”, como, por ejemplo, en la videovigilancia o las *cookies*.

**Título IV**

En él se recogen todos los tratamientos concretos, con especial atención sobre lo relativo a los tratamientos de datos por entidades financieras y en específico, a lo relativo a la morosidad.

**Título V**

En este título se define la figura del responsable y encargado del tratamiento, delimitando las responsabilidades y las valoraciones para adoptar las medidas necesarias para el cumplimiento de la normativa de protección de datos. También se menciona la figura del delegado de protección de datos y los mecanismos de autorregulación y certificación. Dicho delegado puede ser una persona física o jurídica, estar o no dentro de la organización del responsable y puede tener un carácter obligatorio o voluntario y que no podrá ser removido salvo negligencia grave. Será la Agencia Española de protección de datos la encargada de mantener un listado público y actualizado de dichos delegados.

**Título VI**
En él se hace referencia a todo lo relativo a las transferencias internacionales de datos junto con los procedimientos con los que cuentan las autoridades de protección de datos para aprobar dichas transferencias.

**Título VII**
Dicho título está dedicado a las autoridades de protección de datos, reflejando la existencia de autoridades a nivel autonómico y su necesaria cooperación. La Agencia Española de Protección de Datos se configura como una autoridad administrativa independiente.

**Título VIII**
En este título se regulan los procedimientos en caso de que se vulnere la normativa de protección de datos. Se propone un modelo en el que existe una autoridad de control principal y otras autoridades interesadas. También se establece el procedimiento de cooperación entra las distintas autoridades de los Estados miembros de la Unión Europea, siendo la decisión vinculante en caso de discrepancia la del Comité Europeo de Protección de Datos. En caso de que el tratamiento de datos tenga carácter fronterizo, será necesario ver qué autoridad se considera como principal.

**Título IX**
El título IX establece el sistema de sanciones o acciones correctivas en caso de vulnerar el reglamento. Se procede a distinguir entre el tipo de infracciones y su grado: muy graves, graves y leves. Además, se trata la determinación de la cuantía de las sanciones, considerando si existen factores agravantes o reincidencia.

**Título X**
Finalmente, el Título X se destina al reconocimiento y garantía de los derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. En particular, la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital, así como los derechos al olvido, a la portabilidad y al testamento digital. Es de especial relevancia también el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet. Resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones.

## III. Asignación de actividades por artículo

En la siguiente tabla se muestra cada uno de los artículos que se ha considerado que tienen cabida dentro del proceso unificado de desarrollo *software*, indicando a qué actividad o actividades pertenece cada uno.

| Artículo | Captura de requisitos y análisis | Diseño | Implementación y pruebas | Mantenimiento |
|---|---|---|---|---|
| Art. 3 | X | | | X |
| Art. 4 | X | X | | X |
| Art. 5 | | X | | |
| Art. 6 | | | X | |
| Art. 7 | | | X | |
| Art. 8 | X | | | |
| Art. 9 | X | X | | |
| Art. 10 | X | X | | |
| Art. 11 | X | X | X | |
| Art. 12 | X | | X | |
| Art. 13 | X | | X | |
| Art. 14 | X | | X | |
| Art. 15 | X | | X | |
| Art. 16 | X | | X | |
| Art. 17 | X | | X | |
| Art. 18 | X | | X | |
| Art. 19 | X | | | |
| Art. 20 | X | | | |
| Art. 21 | X | | | |
| Art. 22 | X | | | |
| Art. 23 | X | | | |
| Art. 25 | X | | | |
| Art. 28 | X | | | |
| Art. 29 | X | | | |
| Art. 30 | X | | | |
| Art. 31 | X | | | X |
| Art. 32 | X | | | X |
| Art. 33 | X | | | |
| Art. 34 | X | | | |
| Art. 35 | X | | | |
| Art. 36 | X | | | |
| Art. 37 | X | | | |
| Art. 39 | | | | X |
| Art. 40 | | X | | |
| Art. 41 | | X | | |
| Art. 42 | | X | | |
| Art. 43 | | X | | |
| Art. 80 | X | | X | |

| | | | | |
|---|---|---|---|---|
| Art. 82 | | | | |
| Art. 84 | | | | |
| Art. 85 | | | | |
| Art. 87 | | | | |
| Art. 88 | | | | |
| Art. 89 | | | | |
| Art. 90 | | | | |
| Art. 92 | | | | |
| Art. 93 | | | | |
| Art. 94 | | | | |
| Art. 95 | | | | |
| Art. 96 | | | | |

## IV. Artículos sin cabida en alguna de las actividades del desarrollo

En la siguiente tabla se muestran todos aquellos artículos, de los noventa y siete que conforman la LOPDP, que no tienen cabida dentro del proceso *software* por el motivo indicado.

| Artículo | Motivo por el que no aplica en el proceso de desarrollo software |
|---|---|
| Art. 1 | Objeto de la ley |
| Art. 2 | Ámbito de aplicación |
| Art. 24 | Sistemas de denuncias |
| Art. 26 | Tratamientos por parte de Administraciones Públicas |
| Art. 27 | Tratamientos sobre infracciones |
| Art. 38 | Códigos de conducta |
| Art. 44 | Actividades de la Agencia Española de Protección de Datos |
| Art. 45 | Actividades de la Agencia Española de Protección de Datos |
| Art. 46 | Actividades de la Agencia Española de Protección de Datos |
| Art. 47 | Actividades de la Agencia Española de Protección de Datos |
| Art. 48 | Actividades de la Agencia Española de Protección de Datos |
| Art. 49 | Actividades de la Agencia Española de Protección de Datos |
| Art. 50 | Actividades de la Agencia Española de Protección de Datos |
| Art. 51 | Actividades de la Agencia Española de Protección de Datos |
| Art. 52 | Actividades de la Agencia Española de Protección de Datos |
| Art. 53 | Actividades de la Agencia Española de Protección de Datos |
| Art. 54 | Actividades de la Agencia Española de Protección de Datos |
| Art. 55 | Actividades de la Agencia Española de Protección de Datos |
| Art. 56 | Actividades de la Agencia Española de Protección de Datos |
| Art. 57 | Procedimientos autonómicos |
| Art. 58 | Procedimientos transfronterizos |
| Art. 59 | Procedimientos transfronterizos |
| Art. 60 | Procedimientos transfronterizos |
| Art. 61 | Procedimientos transfronterizos |
| Art. 62 | Procedimientos transfronterizos |
| Art. 63 | Régimen sancionador |
| Art. 64 | Régimen sancionador |
| Art. 65 | Régimen sancionador |
| Art. 66 | Régimen sancionador |
| Art. 67 | Régimen sancionador |
| Art. 68 | Régimen sancionador |
| Art. 69 | Régimen sancionador |
| Art. 70 | Régimen sancionador |
| Art. 71 | Régimen sancionador |
| Art. 72 | Régimen sancionador |
| Art. 73 | Régimen sancionador |
| Art. 74 | Régimen sancionador |
| Art. 75 | Régimen sancionador |
| Art. 76 | Régimen sancionador |

| | |
|---|---|
| Art. 77 | Régimen sancionador |
| Art. 78 | Régimen sancionador |
| Art. 79 | Introductorio |
| Art. 81 | Acceso universal a Internet |
| Art. 83 | Educación digital |
| Art. 86 | Derecho a la actualización de la información en medios digitales |
| Art. 91 | Derechos de negociación colectiva |
| Art. 97 | Políticas gubernamentales |

# V. Formulario de cumplimiento del RGPD

A continuación, se muestra el formulario con el listado para el cumplimiento del RGPD [1] creado por la Agencia Española de Protección de Datos [21]. Dicho formulario se ha utilizado para validad la prueba de concepto propuesta en el Capítulo 5, y se indica si cada característica en se cumple, no se cumple o no es pertinente.

| **PRINCIPIOS RELATIVOS AL TRATAMIENTO** | **Tratado en la adaptación (Sí / No / NA)** |
|---|---|
| Se recogen los datos personales con fines determinados | Sí |
| Se recogen los datos personales con fines explícitos | Sí |
| Se recogen los datos personales con fines legítimos | Sí |
| Se tratan ulteriormente de manera incompatible con otros fines | No |
| Los datos personales se mantienen exactos | Sí |
| Se mantienen actualizados | Sí |
| Se rectifican los datos personales inexactos respecto de la finalidad | Sí |
| Se suprimen los datos personales inexactos respecto de la finalidad | Sí |
| Se mantienen durante más tiempo del necesario respecto de la finalidad | Sí |
| Se tratan con fines de archivo en interés público | No |
| Se tratan con fines de investigación científica | No |
| Se tratan con fines históricos | No |
| Los datos personales se tratan con fines estadísticos | No |
| Se han implantado medidas de seguridad para proteger la integridad y confidencialidad de los datos | Sí |
| Se han implantado medidas de seguridad contra el tratamiento no autorizado o ilícito de los datos | Sí |
| Se han implantado medidas de seguridad para evitar su pérdida, destrucción o daño accidental | Sí |
| Se mantiene la trazabilidad de los fines del tratamiento | Sí |

| **LICITUD DEL TRATAMIENTO** | **Tratado en la adaptación (Sí / No / NA)** |
|---|---|
| Se tiene consentimiento para cada finalidad del tratamiento | Sí |
| El tratamiento es necesario para ejecutar un contrato o precontrato | No aplica |
| Existe obligación legal | Sí |
| El tratamiento es necesario para proteger intereses vitales | No aplica |
| El tratamiento es necesario para el cumplimiento de interés público | No aplica |
| El tratamiento es necesario para satisfacer intereses legítimos | No aplica |

| CONDICIONES PARA EL CONSENTIMIENTO | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Se puede demostrar que el afectado dio su consentimiento para el tratamiento | Sí |
| Se puede demostrar que el tratamiento se realiza como resultado del cumplimiento de una obligación legal | Sí |
| Se solicita el consentimiento de forma clara e independiente de los demás asuntos | Sí |
| Se solicita el consentimiento de forma inteligible y de fácil acceso | Sí |
| Se solicita usando lenguaje claro y sencillo | Sí |
| Se informa con carácter previo a recabar el consentimiento | Sí |
| Se permite retirar el consentimiento con la misma facilidad que se recaba | Sí |
| Se ofrecen medios para retirar el consentimiento en cualquier momento | Sí |
| Se recaba el libre consentimiento | Sí |
| Para prestar un servicio se solicitan sólo los datos necesarios | Sí |
| Para ejecutar un contrato se solicitan sólo los datos necesarios | No aplica |

| CONSENTIMIENTO DE NIÑOS EN RELACIÓN CON LOS SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Se recaba el consentimiento de menores de 14 años al titular de la patria potestad o tutela sobre el niño | Sí |
| Se verifica que el consentimiento fue dado por el titular de la patria potestad o tutela sobre el niño | Sí |

| TRATAMIENTO DE CATEGORIAS ESPECIALES DE DATOS | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Se tratan los datos sólo cuando existen normas que lo exceptúen | Sí |
| Se tratan los datos con consentimiento explícito y no existen normas de derecho que prohíban expresamente su tratamiento | Sí |
| Es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la seguridad y protección en la medida que está establecido por las normas de derecho | No aplica |
| Es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la seguridad y protección en la medida que existe un convenio colectivo con arreglo a derecho | No aplica |

| | |
|---|---|
| Es necesario para proteger los intereses vitales de una persona y el interesado no está capacitado, física o jurídicamente, para dar su consentimiento | No aplica |
| Se efectúa en el ámbito de actividades legítimas y con las debidas garantías y se refiere exclusivamente a los miembros actuales o antiguos o a personas que mantienen contactos regulares en relación con la finalidad (política, filosófica, religiosa o sindical) | Sí |
| Se efectúa en el ámbito de actividades legítimas y con las debidas garantías y no se comunican a terceros sin consentimiento de los interesados | Sí |
| Se tratan datos que el interesado ha hecho manifiestamente públicos | Sí |
| Es necesario para la formulación, el ejercicio o la defensa de reclamaciones | No |
| Es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social | No |
| Es necesario por razones de interés público en el ámbito de la salud pública sobre la base normas de Derecho que establece medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional | No |
| Es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos en base a normas de derecho | No |
| Se realiza cumpliendo las condiciones con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud que establece la normativa nacional | No |

| **TRATAMIENTOS RELATIVOS A CONDENAS E INFRACCIONES PENALES** | **Tratado en la adaptación (Sí / No / NA)** |
|---|---|
| Se tratan los datos bajo la supervisión de las autoridades públicas | No |
| Se tratan los datos bajo la autorización de normas de derecho | No |
| El registro completo de condenas penales se realiza bajo el control de las autoridades públicas | No |

| **TRATAMIENTOS QUE NO REQUIEREN IDENTIFICACIÓN** | **Tratado en la adaptación (Sí / No / NA)** |
|---|---|
| Se mantiene información adicional con vistas a identificar al interesado cuando los fines no requieren esa identificación | No |

| | |
|---|---|
| Se obtiene y/o trata información adicional con vistas a identificar al interesado cuando los fines no requieren esa identificación | No |
| Se puede demostrar que los datos anonimizados no permiten identificar a los interesados | No |
| Se informa al interesado y se recaba su consentimiento cuando se llega a su identificación | No |
| Se cancelan los datos cuando se llega a identificar al interesado | No |

| **DERECHOS DEL INTERESADO. TRANSPARENCIA DE LA INFORMACIÓN** | **Tratado en la adaptación (Sí / No / NA)** |
|---|---|
| Se toman medidas para facilitar al interesado toda la información relativa al tratamiento | Sí |
| La información se facilita de forma concisa, transparente e inteligible | Sí |
| La información se facilita en lenguaje claro y sencillo | Sí |
| Se facilita por escrito o por otros medios, incluidos los electrónicos | Sí |
| Se facilita verbalmente, previa acreditación de su identidad | No aplica |
| Se facilita al interesado el ejercicio de sus derechos | Sí |
| Se atienden las peticiones del ejercicio de derechos aunque el tratamiento no requiera identificación salvo que no se pueda identificar al interesado | Sí |
| Se informa al interesado en el plazo de un mes desde la recepción de su solitud | Sí |
| Se informa ante el ejercicio de derechos complejos o ante muchas solicitudes en el plazo máximo de tres meses desde la recepción de la solicitud | No |
| Se informa en el plazo de un mes de la prórroga de tres meses indicando el motivo de la dilación | No |
| Se permite a los interesados el ejercicio de derechos por medios electrónicos | Sí |
| Se informa por medios electrónicos cuando se recibe la solicitud por esos medios salvo que solicite que se realice por otro medio | Sí |
| Se informa de las razones de la no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales, en el plazo de un mes desde la recepción de la solicitud cuando no se da curso a la solicitud | No |
| Se facilita gratuitamente el ejercicio de derechos | Sí |
| Se solicita información para acreditar la identidad de la persona física que ejerce sus derechos | Sí |
| Cuando la información que se facilita utiliza iconos normalizados, el formato electrónico es legible mecánicamente | Sí |

| DERECHOS DEL INTERESADO. INFORMACIÓN A FACILITAR CUANDO LOS DATOS SE OBTIENEN DEL INTERESADO | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Se facilita la identidad y los datos de contacto del responsable y, en su caso, del representante cuando se solicitan datos | Sí |
| Se facilitan los datos de contacto del delegado de protección de datos | Sí |
| Se facilitan los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento | Sí |
| Se facilita información sobre el interés legitimo | Sí |
| Se informa sobre los destinatarios o las categorías de destinatarios | Sí |
| Se informa del plazo de conservación de los datos personales o los criterios utilizados para determinarlo | No |
| Se informa sobre la existencia del derecho a solicitar el acceso, rectificación o supresión, la limitación del tratamiento, a oponerse y el derecho a la portabilidad | Sí |
| Si el tratamiento se basa en el consentimiento se informa de la existencia del derecho a retirarlo en cualquier momento | Sí |
| Se informa del derecho a presentar una reclamación ante una autoridad de control | No |
| Se informa de las cesiones basadas en requisitos legales o contractuales | No |
| Se informa de las cesiones basadas en un requisito necesario para suscribir un contrato | No |
| Se informa de la existencia de decisiones automatizas, elaboración de perfiles, sobre la lógica aplicada, la importancia y consecuencias previstas del tratamiento | No |
| Antes de realizar tratamientos de datos personales para una finalidad distinta de la que fueron recogidos, se informa al interesado y la información abarca esa otra finalidad y cualquier otra información pertinente | No |

| DERECHOS DEL INTERESADO. INFORMACIÓN A FACILITAR CUANDO LOS DATOS NO SE OBTIENEN DEL INTERESADO | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Se informa de la identidad y los datos de contacto del responsable y, en su caso, de su representante | Sí |
| Se informa de los datos de contacto del DPD | Sí |
| Se informa de los fines del tratamiento | Sí |
| Se informa de la base jurídica del tratamiento | No aplica |
| Se informa de las categorías de datos personales de que se trate | Sí |
| Se informa de los destinatarios o las categorías de destinatarios de los datos | Sí |

| | |
|---|---|
| Se informa del plazo durante el cual se conservarán los datos personales | Sí |
| Se informa de los criterios utilizados para determinar este plazo el plazo de conservación cuando no es posible informar del mismo | No |
| Se informa de los intereses legítimos concretos en que se basa el tratamiento | Sí |
| Se informa del derecho a solicitar el acceso a sus propios datos personales | Sí |
| Se informa del derecho a solicitar la rectificación de sus datos | Sí |
| Se informa del derecho a solicitar la supresión | Sí |
| Se informa del derecho a la limitación del tratamiento | Sí |
| Se informa del derecho a oponerse al tratamiento | Sí |
| Se informa del derecho a la portabilidad de los datos | Sí |
| Se informa de la existencia del derecho a retirarlo el consentimiento en cualquier momento | Sí |
| Se informa del derecho a presentar una reclamación ante una autoridad de control | No |
| Se informa de la fuente de la que proceden los datos personales | Sí |
| Si proceden de fuentes de acceso público, se informa de ello | Sí |
| Se proporciona la información antes de un mes | Sí |
| Si los datos personales se utilizan para comunicación con el interesado, se le comunica la información a que tiene derecho en el momento de la primera comunicación | Sí |
| Si está previsto comunicar los datos personales del interesado a otro destinatario, se le comunica la información a más tardar en el momento en que los datos personales son comunicados por primera vez | Sí |
| Se informa al interesado si se realizan tratamientos para finalidades diferentes de la que fueron recogidos | Sí |
| No se informa cuando ya dispone de la información el interesado | Sí |
| No se informa cuando la comunicación de dicha información resulta imposible o supone un esfuerzo desproporcionado | No aplica |
| No se informa porque puede imposibilitar u obstaculizar gravemente el logro de los objetivos del tratamiento, pero se adoptan medidas para proteger los derechos, libertades e intereses legítimos del interesado | No aplica |
| No se informa porque la obtención o la comunicación está expresamente establecida por normas de derecho aplicables | No aplica |
| No se informa porque los datos personales tienen carácter confidencial sobre la base de una obligación de secreto profesional regulada por normas de Derecho | No aplica |

| DERECHOS DEL INTERESADO. DERECHO DE ACCESO | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Se informa respecto a los fines del tratamiento | Sí |
| Se informa de las categorías de datos personales que se tratan | Sí |
| Se informa de los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales | Sí |
| Se informa del plazo previsto de conservación de los datos personales | Sí |
| Se informa de los criterios utilizados para determinar el plazo de conservación | No |
| Se informa del derecho a solicitar la rectificación o supresión de sus datos | Sí |
| Se informa del derecho a solicitar la limitación del tratamiento de los datos | Sí |
| Se informa del derecho a solicitar la oposición al tratamiento | Sí |
| Se informa del derecho a presentar una reclamación ante una autoridad de control | No |
| Se proporciona información sobre el origen de los datos cuando no recogen del propio interesado | Sí |
| Se facilita copia de los datos personales objeto de tratamiento cuando el interesado lo solicita | Sí |
| Se facilita la información en formato electrónico de uso común si lo solicita por medios electrónicos salvo que se facilite otro medio | Sí |

| DERECHOS DEL INTERESADO. DERECHO DE RECTIFICACIÓN | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Se rectifican los datos personales inexactos sin dilación indebida | Sí |
| Se completan los datos personales incompletos teniendo en cuenta los fines del tratamiento | Sí |

| DERECHOS DEL INTERESADO. DERECHO DE | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Se suprimen los datos cuando no son necesarios en relación con los fines para los que fueron recogidos | Sí |
| Se suprimen los datos cuando se retira el consentimiento en que se basa el tratamiento | Sí |
| Se suprimen los datos cuando se opone al tratamiento | Sí |
| Se suprimen los datos cuando han sido tratados ilícitamente | Sí |
| Se suprimen los datos cuando lo exige una obligación legal | Sí |
| Se suprimen los datos cuando se obtienen en relación con la oferta de servicios de la sociedad de la información | Sí |

| DERECHOS DEL INTERESADO. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Se limita el tratamiento durante un plazo para verificar la exactitud de los datos, cuando el interesado impugna su exactitud | No |
| Se limita el tratamiento cuando es ilícito y el interesado se opone a la supresión de sus datos personales y solicita en su lugar la limitación de su uso | Sí |
| Se limita el tratamiento cuando no son necesarios para los fines, pero el interesado los necesita para la formulación, el ejercicio o la defensa de reclamaciones | No |
| Se limita el tratamiento cuando el interesado se opone al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado | No |
| Se informa al interesado cuando se levanta la limitación del tratamiento | No |

| INFORMACIÓN AL INTERESADO ANTE RECTIFICACIÓN, SUPRESIÓN O LIMITACIÓN EN EL TRATAMIENTO | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Se comunican al interesado la rectificación, supresión o limitación en el tratamiento | Sí |

| DERECHOS DEL INTERESADO. DERECHO A LA PORTABILIDAD DE LOS DATOS | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Se facilitan los datos cuando el interesado lo solicita en un formato estructurado, de uso común y lectura mecánica | Sí |
| Se transmiten dichos datos a otro responsable si el tratamiento está basado en el consentimiento o en un contrato | No aplica |
| Se transmiten dichos datos si el tratamiento se efectúe por medios automatizados | No |
| Se transmiten los datos al nuevo responsable que el interesado determina, si es posible técnicamente | No |

| DERECHOS DEL INTERESADO. DERECHO DE OPOSICIÓN | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Se atienden las solicitudes de oposición y se dejan de tratar los datos | Sí |
| Se atienden las solicitudes de oposición, pero no se dejan de tratar los datos por motivos legítimos imperiosos para el tratamiento que prevalecen sobre los intereses, los derechos y las libertades o para la formulación, el ejercicio o la defensa de reclamaciones | No aplica |

| | |
|---|---|
| Se ponen los medios necesarios para que pueda ejercer su derecho a oponerse por medios automatizados | Sí |

| **DERECHOS DEL INTERESADO. DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES** | **Tratado en la adaptación (Sí / No / NA)** |
|---|---|
| No se realizan tratamientos que supongan la toma una decisión basada únicamente en el tratamiento automatizado y que produzca efectos jurídicos | No |
| Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque es necesario para la celebración o la ejecución de un contrato | No |
| Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque están autorizados en Derecho | No |
| Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque se cuenta con el consentimiento explícito | No |
| Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos | No |
| Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan medidas adecuadas para salvaguardar el derecho a obtener intervención humana por parte del responsable | No |
| Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan medidas adecuadas para dar al interesado ocasión de expresar su punto de vista e impugnar la decisión | No |
| Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se cuenta con el consentimiento del interesado | No |
| Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se cuenta con habilitación legal | No |
| Se informa a los interesados acerca de estas decisiones individuales automatizadas y de la habilitación legal de las mismas | No |

| | |
|---|---|
| Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se han tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado | No |

| **RESPONSABILIDAD DEL RESPONSABLE DEL TRATAMIENTO** | **Tratado en la adaptación (Sí / No / NA)** |
|---|---|
| Se tiene en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento para garantizar y poder demostrar que el tratamiento es conforme con el RGPD | Sí |
| Se tienen en cuenta los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas | Sí |
| Se aplican medidas técnicas y organizativas apropiadas | Sí |
| Las medidas se revisan y actualizan cuando es necesario | Sí |
| Se han confeccionado políticas de protección de datos | Sí |
| Se aplican las políticas de protección de datos | Sí |

| **PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO** | **Tratado en la adaptación (Sí / No / NA)** |
|---|---|
| Se analizan las medidas técnicas y organizativas apropiadas antes de determinar los medios de tratamiento | Sí |
| Durante el diseño del tratamiento se tienen en cuenta las medidas técnicas y organizativas apropiadas para cumplir con el RGPD | Sí |
| Durante el tratamiento se aplican las medidas que han sido determinadas | Sí |
| Durante el tratamiento se comprueba la efectividad de las medidas aplicadas | Sí |
| Se aplican medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratan datos necesarios para cada uno de los fines | Sí |
| Se aplican medidas técnicas y organizativas teniendo en cuenta la cantidad de datos personales recogidos, la extensión del tratamiento, el plazo de conservación y la accesibilidad | Sí |
| Las medidas garantizan que, por defecto, los datos no son accesibles a un número indeterminado de personas físicas, sin la intervención de personal | Sí |

| **CORRESPONSABLES DEL TRATAMIENTO** | **Tratado en la adaptación (Sí / No / NA)** |
|---|---|

| | |
|---|---|
| Se han determinado de modo transparente, y de mutuo acuerdo, las responsabilidades respectivas de los corresponsables en el cumplimiento de las obligaciones impuestas por el RGPD | No |
| El acuerdo fija las respectivas obligaciones de suministro de información al interesado | No |
| El acuerdo entre corresponsables del tratamiento refleja las funciones y relaciones respectivas de ambos en relación con los interesados | No |
| Los aspectos esenciales del acuerdo están a disposición del interesado | No |

| **ENCARGADO DEL TRATAMIENTO** | **Tratado en la adaptación (T / P / NA / N)** |
|---|---|
| Se eligen los que ofrecen garantías suficientes conforme con los requisitos del RGPD y garantizando la protección de los derechos del interesado | No aplica |
| El encargado del tratamiento no recurre a otro encargado sin la autorización previa por escrito | No aplica |
| El tratamiento por el encargado se rige por un contrato u otro acto jurídico vinculante con arreglo a las normas de Derecho | No aplica |
| El contrato establece el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados así como las obligaciones y derechos del responsable | No aplica |
| El contrato establece que se tratan los datos personales únicamente siguiendo instrucciones documentadas del responsable | No aplica |
| El contrato garantiza que las personas autorizadas para tratar datos personales se han comprometido a respetar la confidencialidad o están sujetas a una obligación de confidencialidad de naturaleza estatutaria | No aplica |
| El contrato establece que se tomarán las medidas de seguridad necesarias | No aplica |
| El contrato establece que se respetarán las condiciones indicadas para recurrir a otro encargado del tratamiento | No aplica |
| El contrato establece que el encargado asistirá para que se pueda responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados | No aplica |
| El contrato establece que se suprimirán o devolverán los datos personales una vez finalice la prestación de los servicios, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales | No aplica |

| | |
|---|---|
| El contrato establece que pondrá a disposición toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías e inspecciones, por parte del responsable o de otro auditor autorizado por el responsable | No aplica |
| El contrato establece que si el encargado del tratamiento recurre a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se imponen a este otro encargado las mismas obligaciones de protección de datos que las estipuladas en el contrato, mediante contrato u otro acto jurídico establecido con arreglo a Derecho | No aplica |
| El contrato consta por escrito | No aplica |
| Sólo se accede a los datos siguiendo instrucciones del responsable | No aplica |

| **REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO** | **Tratado en la adaptación (Sí / No / NA)** |
|---|---|
| Se lleva un registro de las actividades de tratamiento | Sí |
| El registro recoge el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos | Sí |
| El registro recoge los fines del tratamiento | Sí |
| Recoge una descripción de las categorías de interesados y de las categorías de datos personales | Sí |
| Recoge las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales | Sí |
| Recogen las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional | Sí |
| Incluye los plazos previstos para la supresión de las categorías de datos | No |
| Incluye una descripción general de las medidas técnicas y organizativas apropiadas al riesgo de los tratamientos | Sí |

| **SEGURIDAD DEL TRATAMIENTO** | **Tratado en la adaptación (Sí / No / NA)** |
|---|---|
| Para determinar las medidas a aplicar se tiene en cuenta el estado de la técnica, costes de aplicación, y la naturaleza, alcance, contexto y fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas | Sí |

| | |
|---|---|
| Se aplican las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo | Sí |
| Se han incluido medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento | Sí |
| Medidas para asegurar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico | Sí |
| Existe un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento | Sí |
| Se han tenido en cuenta los riesgos que presenta el tratamiento como consecuencia de su destrucción, pérdida o alteración accidental o ilícita que son transmitidos, conservados o tratados, o la comunicación o acceso no autorizados a dichos datos para evaluar el nivel de seguridad aplicado | Sí |
| Se han tomado medidas para garantizar que las personas autorizadas a acceder a datos sólo los tratan siguiendo instrucciones | Sí |

| **NOTIFICACIÓN DE BRECHAS DE LA SEGURIDAD DE LOS DATOS PERSONALES A LA AUTORIDAD DE CONTROL** | **Tratado en la adaptación (Sí / No / NA)** |
|---|---|
| Se ha establecido un procedimiento para identificar y gestionar las brechas de seguridad | Sí |
| Existe un procedimiento para que los encargados del tratamiento notifiquen las brechas al responsable en el momento en que tengan conocimiento de ellas | No |
| Existe un procedimiento para notificar a la autoridad de control en el plazo de 72 horas | No |
| Existe un procedimiento para documentar los motivos por los que no se puede notificar en el plazo de 72 horas | No |
| Existe un procedimiento para facilitar la información de manera gradual cuando no es posible facilitarla simultáneamente | No |
| Se documenta cualquier brecha de seguridad de los datos personales | Sí |
| En la documentación se incluyen los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas | Sí |
| Se ha comprobado que el procedimiento de notificación funciona | No |

| COMUNICACIÓN DE UNA BRECHA AL INTERESADO | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Existe un procedimiento para comunicar la brecha sin dilación indebida cuando sea probable que entrañe un alto riesgo para los derechos y libertades | No |
| La comunicación al interesado, se lleva a cabo en un lenguaje claro y sencillo, describe la naturaleza de la brecha | No |

| EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Se recaba el asesoramiento del DPD | No aplica |
| Se realiza EIPD antes del tratamiento cuando es probable que entrañe un alto riesgo para los derechos y libertades de las personas | No aplica |
| Se realiza una EIPD antes en tratamientos a gran escala de categorías especiales de datos o relativos a condenas e infracciones penales | No aplica |
| Se realiza una EIPD antes de tratamiento que suponen una observación sistemática a gran escala de una zona de acceso público | No aplica |
| Se realiza una EIPD en operaciones de tratamiento incluidas en la lista publicada por la autoridad de control | No aplica |
| La EIPD incluye una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, y cuando procede el interés legítimo perseguido | No aplica |
| Incluye una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad | No aplica |
| La EIPD incluye una evaluación de los riesgos para los derechos y libertades | No aplica |
| Incluye medidas previstas para demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas | No aplica |
| Incluye las medidas previstas para afrontar los riesgos, garantías y mecanismos para garantizar la protección de datos | No aplica |
| Se reexaminan las EIPD siempre que es necesario y cuando exista un cambio de los riesgos que representen las operaciones de tratamiento | No aplica |
| Se consulta a la autoridad de control antes de proceder al tratamiento cuando una EIPD muestre que el mismo entrañaría un alto riesgo si no se toman medidas para mitigarlo | No aplica |
| Se informa de las responsabilidades respectivas de los implicados en el tratamiento en la consulta a la autoridad de control | No aplica |

| | |
|---|---|
| Se informa de los fines y medios del tratamiento previsto en la consulta | No aplica |
| Se informa de las medidas y garantías establecidas para proteger los derechos y libertades en la consulta | No aplica |
| Se facilitan los datos de contacto del delegado de protección de datos | No aplica |
| Se incluye la evaluación de impacto | No aplica |
| Cuando se consulta se facilita cualquier información adicional que solicite la autoridad de control | No aplica |

| **DELEGADO DE PROTECCIÓN DE DATOS** | **Tratado en la adaptación (Sí / No / NA)** |
|---|---|
| Se ha designado un DPD por requerimiento legal | No aplica |
| Se ha designado un DPD atendiendo a sus cualidades de profesionalidad, conocimientos y competencias en la materia | No aplica |
| Se han publicado los datos de contacto del DPD y se ha comunicado a la autoridad de control | No aplica |
| Se garantiza que el DPD participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales | No aplica |
| Se da respaldo en el desempeño sus funciones | No aplica |
| Se le facilitan los recursos necesarios para el desempeño de sus funciones, el acceso a los datos personales y a las operaciones de tratamiento | No aplica |
| Se le facilitan los recursos necesarios para mantener sus conocimientos | No aplica |
| Se garantiza que el DPD no recibe ninguna instrucción en lo que respecta al desempeño de sus funciones | No aplica |
| No se puede destituir ni sancionar al DPD por desempeñar sus funciones | No aplica |
| El DPD rinde cuentas directamente al más alto nivel jerárquico | No aplica |
| El DPD atiende las solicitudes de los interesados | No aplica |
| El DPD está obligado a mantener la confidencialidad en el desempeño de sus funciones | No aplica |
| Si el DPD desempeña otras funciones, se garantiza que no dan lugar a conflicto de intereses | No aplica |
| Las funciones del DPD son informar, asesorar y formar al personal de las obligaciones que les incumben | No aplica |
| El DPD coopera y actúa como punto de contacto con la autoridad de control | No aplica |

| TRANSFERENCIAS A PAÍSES TERCEROS U ORGANIZACIONES INTERNACIONALES | Tratado en la adaptación (Sí / No / NA) |
|---|---|
| Se realizan transferencias a países, o sectores de los mismos, u organizaciones internacionales declarados de nivel de protección adecuado por la Comisión Europea | Sí |
| Se realiza un seguimiento de la validez de las decisiones de adecuación de la Comisión europea | No aplica |
| Se realizan transferencias mediante garantías adecuadas que ofrezcan a los interesados derechos exigibles y posibilidad de acciones legales. | Sí |
| Existe un instrumento jurídico vinculante y exigible entre las autoridades u organismos públicos | No aplica |
| Existen normas corporativas vinculantes | No aplica |
| Existen cláusulas tipo de protección de datos adoptadas por la Comisión | No aplica |
| Existen cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión | No aplica |
| Existe un código de conducta junto con compromisos vinculantes y exigibles en el tercer país que permita aplicar garantías adecuadas | No aplica |
| Existe un mecanismo de certificación junto con compromisos vinculantes y exigibles en el tercer país que permita aplicar garantías adecuadas | Sí |
| Existen cláusulas contractuales que requieren la autorización previa de la autoridad de control | No aplica |
| Existen acuerdos administrativos entre autoridades y organismos públicos que incorporen disposiciones que incluyan derechos efectivos y exigibles para los interesados | No aplica |
| Se realizan transferencias internacionales en ausencia de decisión de adecuación de la Comisión europea y de garantías adecuadas | No aplica |
| Se dispone del consentimiento explícito del interesado y se le ha informado de los posibles riesgos | Sí |
| Son necesarias para la ejecución de un contrato con el interesado o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado | No aplica |
| Son necesarias para la formulación, ejercicio o la defensa de reclamaciones | No aplica |
| Son necesarias para la protección de los intereses vitales del interesado o de otras personas, cuando el interesado esté incapacitado para dar su consentimiento | No aplica |
| Por intereses legítimos imperiosos | No aplica |
| Afecta a un número limitado de interesados y no es repetitiva | No aplica |
| Se han evaluado todas las circunstancias concurrentes y se han ofrecido garantías apropiadas | No aplica |
| Se ha informado a la autoridad de control | No aplica |